Université Abou Bekr Belkaid
جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Université Abou BakrBelkaid- Tlemcen-
Faculté des sciences
Département d'informatique

Mémoire de fin d'études
Pour l'obtention du diplôme d'Ingénieur d'État en Informatique

Option : Système d'information avancé

Thème :

LA SECURITE DU PROTOCOLE OLSR DANS LES RESEAUX AD HOC

Présenté par :

- ✓ BOUCHACHIA Abdelmadjid
- ✓ BOUDJERAD Zouhir

Devant le jury composé de :

• Mr MERZOUG Mohammed	Président
• Mr MOUSSAOUI Djilali	Examinateur
• Mr BELABED Amine	Examinateur
• Mr. KADRI Benamar	Encadreur

Année universitaire 2010/2011

Sommaire

Chapitre III

Chapitre IV

Résumé

Les réseaux sans fil ad hoc ou MANET, *Mobile Ad hoc NETwork,* sont des réseaux dont la Topologie ne bénéficie d'aucune infrastructure préexistante. Elle se forme au gré de l'apparition et du mouvement des nœuds.

L'évolution rapide des performances des réseaux locaux sans fil et leur utilisation de plus en plus importante par les utilisateurs mobiles devraient bénéficier au développement des MANET. Si les MANET se différencient des réseaux classiques, cellulaires ou filaires, par les caractéristiques de leur topologie, les services demandés au réseau par les utilisateurs restent identiques, notamment en matière de sécurité.

Ce mémoire examine les problématiques de sécurité liées à la protection du routage dans les réseaux ad hoc (MANETs). La thèse classifie les différentes attaques qui peuvent être portées et examine en détail le cas du protocole OLSR (Optimized Link State Routing). Une architecture de sécurisation basée sur l'ajout d'une signature numérique est étudiée. D'autres contre-mesures plus élaborées sont également présentées.

Les mécanismes de sécurité sont renforcés par un système de détection d'intrusions distribué et coopératif. Chaque nœud est équipé d'un IDS, *Intrusion Détection System,* local et des agents mobiles autonomes sont mis en œuvre, si nécessaire, pour collecter les informations stockées sur les autres nœuds.

Mots-clés : Manet, routage, OLSR, sécurité, signature numérique

Liste des figures

Liste des tableaux

Introduction générale

Les technologies sans fil occupent aujourd'hui une place prépondérante dans notre vie professionnelle et personnelle et nous permettent de cumuler, de traiter et de distribuer de l'information d'une manière ubiquitaire. Le développement soutenu des réseaux sans fils de ces dernières années se comprend bien au regard des atouts des objets communicants par ce biais. De plus, les applications touchent différents domaines tels les réseaux tactiques militaires, la protection civile ou encore l'étude de l'environnement. Les réseaux ad hoc sont des réseaux sans fils qui ont la capacité de s'auto-organiser, sans la nécessité d'avoir une infrastructure fixe. Lorsque des nœuds entrent en communication dans un réseau ad hoc, le réseau ne possède pas, a priori, de moyen permettant les communications entre des nœuds non voisins. Le groupe MANET de 1' IETF fournit une définition plus précise en introduction de RFC3626 : « Un réseau ad hoc comprend des plates-formes mobiles (par exemple, un routeur interconnectant différents hôtes et équipement sans fil) appelées nœuds qui sont libres de se déplacer sans contraintes. Un réseau ad hoc est donc un système autonome de nœuds mobiles.

Ce système peut fonctionner d'une manière isolée ou s'interfacer à des réseaux fixes au travers de passerelles. Dans ce dernier cas, un réseau ad hoc est un réseau d'extrémité.» Il n'en reste pas moins que la terminologie « réseau ad hoc » est relativement peu explicite. C'est sans doute la raison pour laquelle la communauté scientifique la remplace parfois par celle de « réseau spontané », traduction de *spontaneous network*. A partir de cette définition générale, il est intéressant de mettre en avant les caractéristiques principales qui différencient un réseau ad hoc d'un réseau classique. Mobilité : La mobilité des nœuds constitue à l'évidence une caractéristique très spécifique des réseaux ad hoc. Cette mobilité est intrinsèque au fonctionnement du réseau. Elle se distingue de la nomadicité (mobilité des seuls nœuds terminaux) ou de l'itinérance (équipements statiques mais pouvant être déplacés).

Dans un réseau ad hoc, la topologie du réseau peut changer rapidement, de façon aléatoire et non prédictible et les techniques de routage des réseaux classiques, basées sur des routes préétablies, ne peuvent plus fonctionner correctement. Equivalence des nœuds du réseau : Dans un réseau classique, il existe une distinction nette entre les nœuds terminaux (stations, hôtes) qui supportent les applications et les nœuds internes (routeurs par exemple) du réseau, en charge de l'acheminement des données. Cette différence n'existe pas dans les réseaux ad hoc car tous les nœuds peuvent être amenés à assurer des fonctions de

routage. Liaisons sans fil : Les technologies de communication sans fil sont indispensables à la mise en place d'un réseau ad hoc. Malgré des progrès très importants, leurs performances restent et resteront en deçà de celles des technologies des réseaux filaires. La bande passante est moins importante, alors que le routage et la gestion de la mobilité génèrent davantage de flux de contrôle et de signalisation que dans une architecture de réseau filaire.

Ces flux doivent être traités de façon prioritaire pour prendre en compte rapidement les modifications de topologie. Autonomie des nœuds : La consommation d'énergie constitue un problème important pour des équipements fonctionnant grâce à une alimentation électrique autonome. Ces équipements intègrent des modes de gestion d'énergie et il est important que les protocoles mis en place dans les réseaux ad hoc prennent en compte ce problème. Vulnérabilité : Les réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité. Pour les réseaux ad hoc, le principal problème ne se situe pas tant au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau. Les possibilités de s'insérer dans le réseau sont plus grandes, la détection d'une intrusion ou d'un déni de service plus délicate et l'absence de centralisation pose un problème de remontée de l'information de détection d'intrusions.

Les protocoles de routage permettent de structurer les réseaux ad hoc en maintenant à jour les tables de routage au sein de chaque nœud. Ainsi, un nœud peut joindre un nœud non voisin en le faisant router par des nœuds plus proches. Les informations que le protocole de routage échange (qui sont des informations de contrôle) doivent être sécurisées : II est sinon possible de gêner les communications en injectant de fausses routes, de faux nœuds... Ce projet de fin d'études entre dans ce contexte et il s'intéresse à l'étude de la sécurité du routage, plus précisément la sécurité du protocole proactif OLSR dans le réseau ad hoc.

Ce rapport est organisé comme suit : dans le premier chapitre, nous présentons les différents types de réseaux sans fil ainsi qu'une classification de ces réseaux. Comme on ne peut pas parler de la sécurité d'OLSR sans parler des autres protocoles, le deuxième chapitre donne un aperçu sur les différents types de protocoles de routage existants pour les réseaux ad hoc. Une description générale du protocole OLSR sera faite dans le troisième chapitre. Le quatrième chapitre s'intéresse aux attaques liées au protocole OLSR. Un état de l'art des solutions proposées pour contrer ces attaques fera l'objet de la fin de ce chapitre.

Chapitre I

Présentation générale des réseaux Ad hoc

I.1. Introduction

Les équipements mobiles deviennent de plus en plus petits et puissants en terme de capacité de traitement et de stockage de données. Ainsi, ils sont dotés d'une multitude de fonctionnalités qui permettent d'assurer différents types d'applications et de services.

Ces appareils mobiles, associés aux interfaces du réseau sans fil, sont susceptibles de devenir une partie dominante des infrastructures de l'informatique du futur avec le progrès des techniques de communication sans fil, mobilité et portée. Les réseaux Ad hoc s'inscrivent dans cette nouvelle génération de technologies qui, grâce à la flexibilité qu'ils offrent, fait l'objet d'un engouement certain.

Ce chapitre permet de présenter un panorama général sur les réseaux Ad hoc. Dans un premier temps, nous décrivons le concept de ces réseaux, leurs caractéristiques et les contraintes liées à tel environnement, leurs domaines d'applications, les avantages et les inconvénients qu'ils présentent en introduisant une comparaison avec les autres technologies sans fils. Quelques exemples de réseaux sans fils fonctionnant en mode Ad hoc seront ainsi présentés. On parlera ensuite du problème de routage et l'inadaptation des techniques conventionnelles, et enfin nous donnerons un aperçu sur la qualité de service et la sécurité à travers ces réseaux.

I.2. Définition d'un réseau Ad hoc

L'ambition vouée des réseaux Ad hoc est d'étendre la notion de mobilité pour permettre l'accès à l'information et à la communication n'importe où et n'importe quand. Ces réseaux, si on tente d'en apporter une définition, se caractérisent par un ensemble de stations pouvant être mobiles (topologie dynamique et libre) interconnectées et communiquant entre elles, de manière autonome, via une interface radio ou infrarouge, sans nécessiter d'infrastructures préexistantes. Chaque station a, par ailleurs, le même rôle (administration distribuée), et peut être mise à contribution par d'autres stations pour effectuer le relais des données.

Les unités mobiles ayant un rayon d'émission des signaux de données restreint, un nœud du réseau peut communiquer directement avec ses voisins, c'est-à-dire ceux qui sont à sa portée (on parle alors de communications Ad hoc simple saut), passer par des stations intermédiaires afin d'atteindre sa destination (on parle alors de communications Ad hoc multi saut). Etant donné que chaque nœud du réseau est mobile, il se peut qu'un des nœuds disparaisse, il est donc important que le protocole qui gère l'acheminement des paquets soit très robuste et très adaptable.

Les réseaux Ad hoc sont ceux décrits et étudiés par le groupe de travail Mobile Ad-hoc NETworks (MANET) de l'Internet Engineering Task Force (IETF). Une définition de ces réseaux est

donnée formellement dans le RFC 2501 [1]. La figure (I.1) montre un exemple de réseau Ad hoc utilisant plusieurs relais, les deux nœuds mobiles (A et B) ne peuvent pas communiquer directement. Des relais différents vont acheminer les paquets de la source à la destination, donc un choix de la meilleure route sera nécessaire.

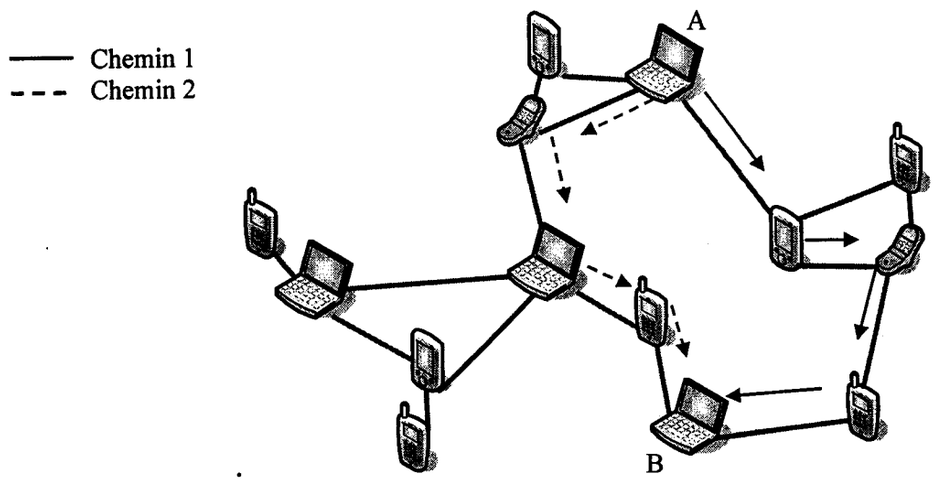


Figure I.1 : Exemple d'un réseau Ad hoc

I.3. Caractéristiques des réseaux Ad hoc

Les réseaux Ad hoc héritent des mêmes propriétés et problèmes des réseaux sans fil. En plus du fait que le canal radio soit limité en termes de bande passante et sujet à un grand taux d'erreurs, ce qui engendre des liaisons à capacité fluctuante.

D'autres caractéristiques spécifiques aux réseaux Ad hoc conduisent à une complexité et des contraintes supplémentaires, qui doivent être prises en compte lors la conception des algorithmes et des protocoles réseaux [1], à savoir :

- L'absence d'une infrastructure centralisée

Les réseaux Ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructure préexistante et de tout genre d'administration centralisée. Chaque noeud travaille dans un environnement pair à pair distribué, et agit en tant que routeur pour relayer des communications, ou pour générer ses propres données. La gestion du réseau est ainsi distribuée sur l'ensemble des éléments du réseau.

- L'auto- configuration

L'auto-configuration permet aux noeuds de s'intégrer facilement dans un réseau. Elle facilite la gestion du réseau car l'interconnexion des éléments ne nécessite qu'un minimum d'intervention technique externe. Cette fonctionnalité est de plus en plus nécessaire pour un déploiement à grande échelle des réseaux sans fil Ad hoc.

- L'impossibilité de mettre en place un plan d'allocation des fréquences

Dans les réseaux sans fil cellulaires, caractérisés par l'utilisation des stations de base, on cherche à attribuer des fréquences différentes aux stations voisines, de telle façon à éviter les interférences entre les cellules ainsi crées. Pour garantir la connectivité, au sein d'un réseau Ad hoc, comme il n'y a pas d'infrastructure fixe et que tous les noeuds sont susceptibles de bouger ou de

disparaître, il est plus simple et moins coûteux de travailler avec une seule fréquence et un multiplexage TDD (Time Division Duplex). La réutilisation spatiale reste possible, mais un noeud qui émet empêche l'accès au canal radio pour tous les mobiles se trouvant dans un voisinage étendu autour de lui, ce qui n'est pas intéressant du tout.

- La mobilité des noeuds et maintenance des routes

La mobilité continue des nœuds crée un changement dynamique de topologie. Par exemple, un noeud peut joindre un réseau, changer de position ou quitter le réseau. Cette mobilité aura un impact direct sur la morphologie du réseau, elle peut engendrer une modification du comportement du canal de communication et en général provoque des influences significatives sur les performances du réseau. Les algorithmes de routage doivent, donc, être capables de résoudre ces problèmes, supporter la maintenance des routes et prendre en charge, en un temps limité, leur reconstruction tout en minimisant l'overhead généré par les messages de contrôle.

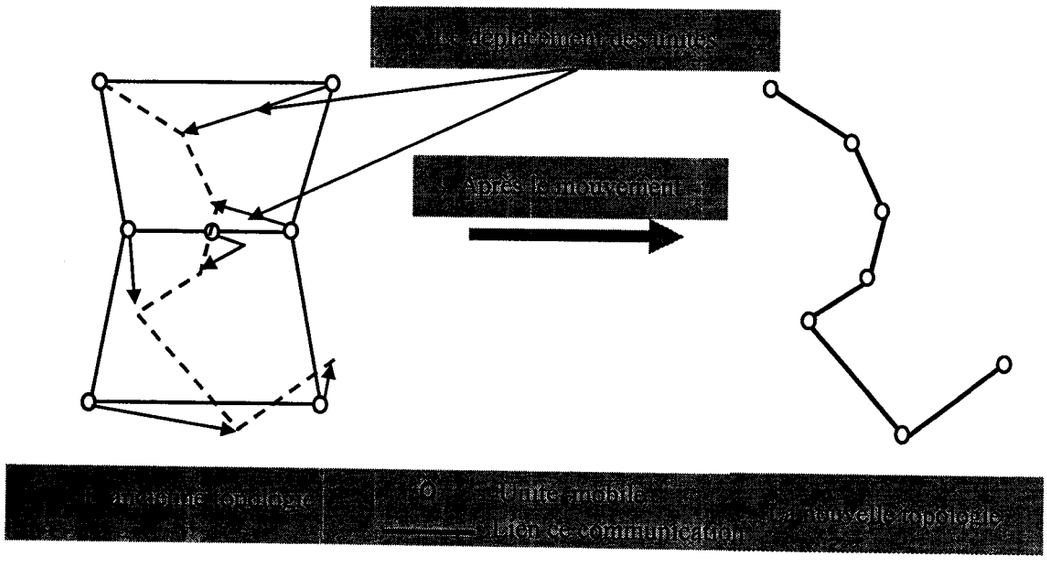


Figure I.2 : Le changement de la topologie des réseaux Ad hoc

- L'hétérogénéité des noeuds

Les nœuds dans un réseau Ad hoc peuvent être équipés d'une ou plusieurs interfaces radio ayant des capacités de transmission variées et opérant dans des plages de fréquences différentes. Cette hétérogénéité de capacité peut engendrer des liens asymétriques dans le réseau. De plus, ces noeuds peuvent avoir des différences, en terme de capacité de traitement (CPU, mémoire), de logiciel, de débit (faible, grand) et de mobilité (lent, rapide). Dans ce cas, une adaptation dynamique des protocoles s'avère nécessaire pour supporter de telles situations.

- La contrainte d'énergie

Une partie des noeuds d'un réseau Ad hoc, voir l'ensemble des noeuds, peut reposer sur des batteries ou un autre moyen limité pour puiser leur énergie. De plus, suivant la topologie du réseau, certains mobiles peuvent se trouver dans des positions clefs et sont appelés à assurer le routage pour un grand nombre de flux (entre plusieurs sous-parties du réseau indépendantes par exemple). Ces noeuds peuvent être amenés à consommer très vite leurs ressources énergétiques. Pour ces noeuds, le

plus important est, sans doute, de mettre en place des critères d'optimisation pour la conservation au maximum de l'énergie, pour éviter d'incessantes recharges du système qui diminue sa mobilité.

- La taille des réseaux Ad hoc

Elle est souvent de petite ou moyenne taille, par exemple dans le cas où le réseau est utilisé pour étendre, temporairement un réseau filaire, comme pour une conférence. Cependant, quelques applications des réseaux Ad hoc nécessitent une utilisation allant jusqu'à des dizaines de milliers de noeuds, comme dans les réseaux de capteurs (Sensor Network) [2]. Des problèmes liés au passage à l'échelle tels que : l'adressage, le routage, la gestion de la localisation des capteurs, la sécurité et sa configuration, doivent être résolus pour une meilleure gestion du réseau.

- Sécurité physique limitée

Dans les réseaux Ad hoc, non seulement les données sont vulnérables comme dans tout réseau radio, mais il en est de même pour le trafic de contrôle et de gestion du routage . Les problématiques de la sécurité dans les réseaux Ad hoc sont donc très complexes, puisque l'on cherche à autoriser de nouveaux mobiles à participer au réseau, tout en évitant des noeuds "malins" qui détourneraient ou perturberaient le fonctionnement même du routage.

Notons cependant un avantage dans le fait que le contrôle des réseaux Ad hoc soit décentralisé, évitant ainsi les problèmes pouvant survenir sur les points centraux dans des approches plus centralisées.

- La qualité de service

De nombreuses applications ont besoin de certaines garanties relatives par exemple au débit, au délai ou encore à la gigue. Dans ces réseaux Ad hoc, ces garanties sont très difficiles à obtenir. Ceci est dû à la nature du canal radio d'une part (interférences et taux d'erreur élevés) et au fait que les "liens" entre les mobiles peuvent avoir à se partager les ressources (alors qu'en filaire, deux liens sont par définition indépendants). De ce fait, les protocoles de qualité de service habituels (par exemple IntServ / RSVP ou Diff-Serv) ne sont pas utilisables directement dans les réseaux Ad hoc et des solutions spécifiques doivent être proposées [3].

I.4. Avantages et inconvénients des réseaux Ad hoc

Indépendamment du fait de disposer ou non d'une infrastructure, le mode Ad hoc multi-saut, comparé aux autres types de réseaux, en particulier les modes de communication avec stations de base, a de nombreux avantages, on peut en citer par exemple :

✓ ***La facilité de déploiement***

La facilité de déploiement est un avantage dans certaines circonstances, comme dans le cas, où on ne dispose pas, ou plus, d'une infrastructure de communications, il suffit de penser aux zones victimes d'une catastrophe naturelle (tremblement de terre). Un bon exemple en a été donné après les attentats du 11 septembre, où les sauveteurs ont pu utiliser comme réseau de communication d'urgence le réseau maillé « Ricochet » dont quelques relais (situés sur des lampadaires) subsistaient dans la zone dévastée; ce réseau est de type Ad hoc [4].

✓ **Le concept de réseau Ad hoc est indépendant des fréquences radio utilisées**

On a vu apparaître plusieurs projets utilisant des bandes de fréquences différentes pour organiser des réseaux Ad hoc. BT (British Telecommunication) mène une expérimentation à l'université de Cardiff avec la solution "Mesh-Works" de la société Radiant Networks. Cette solution travaille dans les bandes des 28 ou 40 GHz, les modulations utilisées étant la QPSK (Quadrature Phase Shift Keying), les 16 ou 64 QAM (Quadrature Amplitude Modulation). De même, le système Ricochet de Metricom utilisait plusieurs bandes de fréquences : 900 MHz, 2.3 et 2.4 GHz, avec GMSK (Gaussian Minimum Shift Keying) comme modulation. D'autres solutions (dont Nokia Rooftop) utilisent les bandes sans licences de 2.4 GHz (bande ISM) ou 5 GHz (bande UNII) dans lesquelles opèrent les interfaces 802.11 (a ou b). Les cartes radio mettant en oeuvre cette norme sont peu chères et d'utilisation aisée [4].

✓ ***La robustesse du réseau***

Les réseaux Ad hoc ont une très grande robustesse puisque pour qu'un réseau local Ad hoc s'effondre, il faudrait qu'un nombre important de machines qui le compose cesse de fonctionner. En effet si l'un des éléments du réseau devient indisponible, cela ne change rien, ou presque, pour les autres, de nouvelles routes vont être crées puis empruntées pour acheminer les données comme si l'élément ne fonctionnant plus n'avait jamais existé. Contrairement au réseau sans fil à architecture cellulaire où tout dépend de l'état du point d'accès, étant donné que toute communication passe par lui.

En outre, les réseau sans fil, sont limités en matière d'obstacles : un mur épais, par exemple, peut stopper une connexion WiFi (Wireless Fidelity) si le point d'accès se trouve de l'autre coté du mur. Dans un réseau Ad hoc, si le récepteur se trouve de l'autre coté du mur, l'émetteur va chercher à établir une connexion en passant par un ou plusieurs nœuds intermédiaires afin de contourner le mur (figureI.3). Dans un réseau Ad hoc, les obstacles physiques ne sont plus un frein à l'établissement du réseau. Ce type de réseau paraît donc bien adapté au milieu urbain.

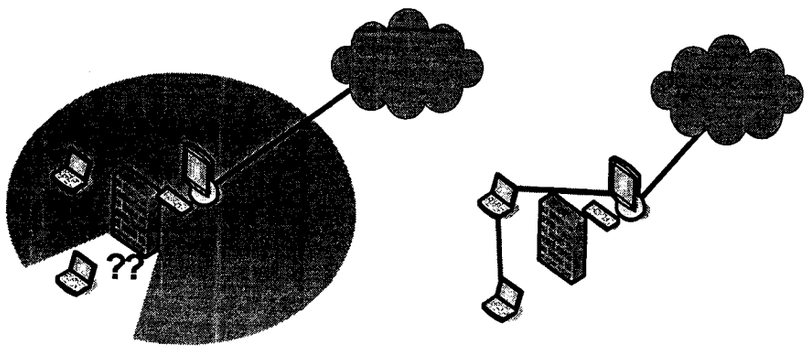


Figure I.3 : La robustesse du réseau Ad hoc vis à vis des obstacles

✓ ***La capacité***

Qu'ont les nœuds d'un réseau Ad hoc servir de routeur, ce type de réseau est intéressant en mode paquet, pour des trafics alternants, périodes d'activités et périodes inactives où l'interface radio peut être utilisée pour router le trafic des autres nœuds [4].

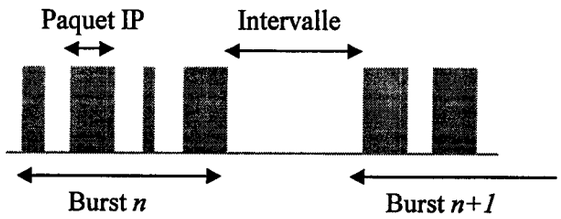


Figure I.4 : Modèle de trafic par bursts

Cependant, les réseaux Ad hoc présentent, comme même, quelques aspects négatifs :

- ***L'inefficacité du système à promouvoir la qualité de service***

Pour rejoindre le destinataire à partir de l'émetteur, les données vont, peut être traverser de nombreuses machines, et chaque relais traversé apporte un délai supplémentaire. Les réseaux Ad hoc ont donc, dans la plupart des cas, une latence plus importante que les réseaux sans fils cellulaires.

- ***Multi- fonctionnalité des stations***

Les machines servant de relais utilisent leurs ressources (batterie, carte réseau sans fil, etc.) pour acheminer des données qui ne les concernent pas, en retour d'autres machines font de même pour leurs transmissions. Ceci entraîne aussi un problème évident de confidentialité puisque tous les éléments coopèrent de manière à acheminer les données y compris des machines (utilisateurs) inconnues d'ou la nécessité d'utiliser des outils de cryptage.

I.5. Les applications des réseaux Ad hoc

Les réseaux Ad hoc sont idéaux pour les applications caractérisées par une absence (ou la non fiabilité) d'une infrastructure préexistante, Ils peuvent exister temporairement pour répondre à un besoin ponctuel de communication. Les applications de tels réseaux sont nombreuses et tendent à se multiplier d'une part avec la miniaturisation des processeurs et la diversité des terminaux, et d'autre part avec l'avancement des recherches dans le domaine des réseaux et l'émergence des technologies sans fil (Bluetooth, IEEE 802.11 et Hiperlan), On distingue :

- Le travail collaboratif et les communications dans des entreprises ou des bâtiments, dans le cadre d'une réunion ou d'une conférence par exemple, les bases de données parallèles, l'enseignement à distance, les systèmes de fichiers répartis;
- Les Applications commerciales : pour un paiement électronique distant (taxi) ou pour l'accès mobile à l'Internet, ou le service de guide par satellites;
- Les Réseaux en mouvement : informatique embarquée et véhicules communicants (sécurité routière, poursuite et détection radar, contrôle de la congestion en temps réel du trafic) ;
- Les services d'urgence : opérations de recherche et de secours des personnes, tremblement de terre, feux, inondation, dans le but de remplacer l'infrastructure fixe détériorée,
- Les Applications domestiques dans les réseaux personnels (WPAN : Wireless Personal Area Network) : le contrôle à distance, via une PDA (Personal Digital Assistant), des équipements divers : téléphone, TV et systèmes d'alarme;
- Les Réseaux de capteurs : pour des applications environnementales (climat, activité de la terre, suivi des mouvements des animaux, . . . etc.)

➢ Applications militaires : sans surprise, les premiers utilisateurs de réseaux Ad hoc ont été les militaires, dont ils présentent aussi un intérêt certain, en particulier pour des réseaux tactiques déployés sur un théâtre d'opérations : communications entre unités mobiles, entre les soldats…etc. La particularité ici c'est la nature du domaine qui exige : de sécurité élevée, de grande capacité, longue durée de vie des batteries et l'intégration d'autres services (GPS …).

➢ Extension de la couverture d'un réseau cellulaire : par exemple dans un WLAN (Wireless local Area Network), un terminal peut communiquer avec une AP (Access point), s'il est hors de sa portée, par l'intermédiaire des stations d'un réseau Ad hoc multi-hop.

I.6. Les réseaux Ad hoc et les autres technologies sans fil

I.6.1. Comparaison des réseaux Ad hoc avec les réseaux cellulaires

Dans un réseau cellulaire, chaque point d'accès couvre une certaine zone géographique (cellule). Pour communiquer entre elles les machines doivent d'abord passer par ces points d'accès, qu'elles soient ou non dans la même cellule. Cela induit que si l'un des points d'accès devient indisponible, tous les équipements se trouvant dans la zone géographique couverte par ce point d'accès, ne peuvent plus communiquer. L'ambition des réseaux Ad Hoc est de supprimer cette notion de point d'accès, ou plus exactement de transformer tous les équipements en points d'accès. Le tableau I.1 présente quelques points de différence entre ces deux types de réseaux.

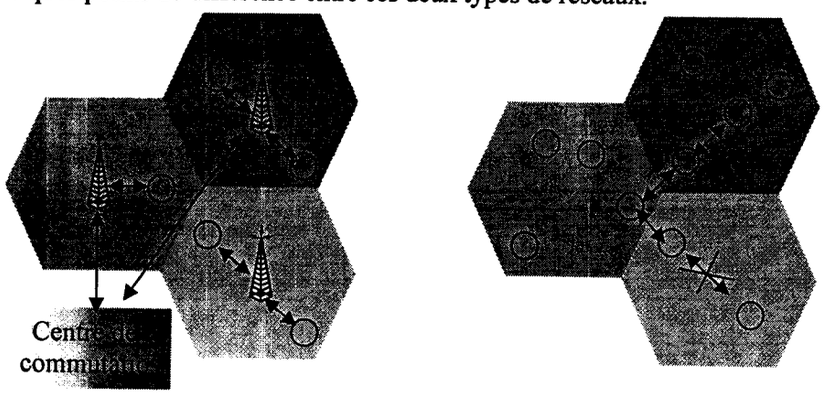


Figure I.5 : Comparaison entre les réseaux Ad hoc et les réseaux cellulaires

Réseaux cellulaires	Réseaux Ad hoc
Infrastructure fixe et administration centralisée	Sans infrastructure et administration distribuée
Liaisons avec simple saut	Liaisons avec simple et multi-saut
Constant Bit Rate est garanti	Canal radio partagé
Initialisés par commutation de circuits	Initialisés par commutation de paquets
Faible déconnexion par l'utilisation du handover	Déconnexion fréquente
Coûts élevés et temps important pour le déploiement	Déploiement vite et peu coûteux
Réutilisation des fréquences et des canaux radio	Allocation dynamique des fréquences et sans réutilisation
La bande de fréquence est assurée facilement	Complexité de la couche MAC
Maintenance coûteuse	Opérations de maintenance intégrées
Equipements moins complexes	Intelligence des équipements pouvant être nécessaire

Tableau I.1 : Comparaison des réseaux Ad hoc et les réseaux cellulaires

I.6.2. Intégration des réseaux Ad hoc dans les réseaux 4G [5]

L'objectif des réseaux de télécommunication 4ème génération (4G), qui sont des réseaux hybrides intègrent différentes topologies et plates-formes réseaux et ciblent la convergence entre le réseau de 3ème génération (UMTS) et les divers standards de réseaux sans fils, puis de fournir aux utilisateurs des services sans interruption dans un environnement hétérogène, indépendamment de leurs positions, du temps et en utilisant des équipements différents en terme de capacité.

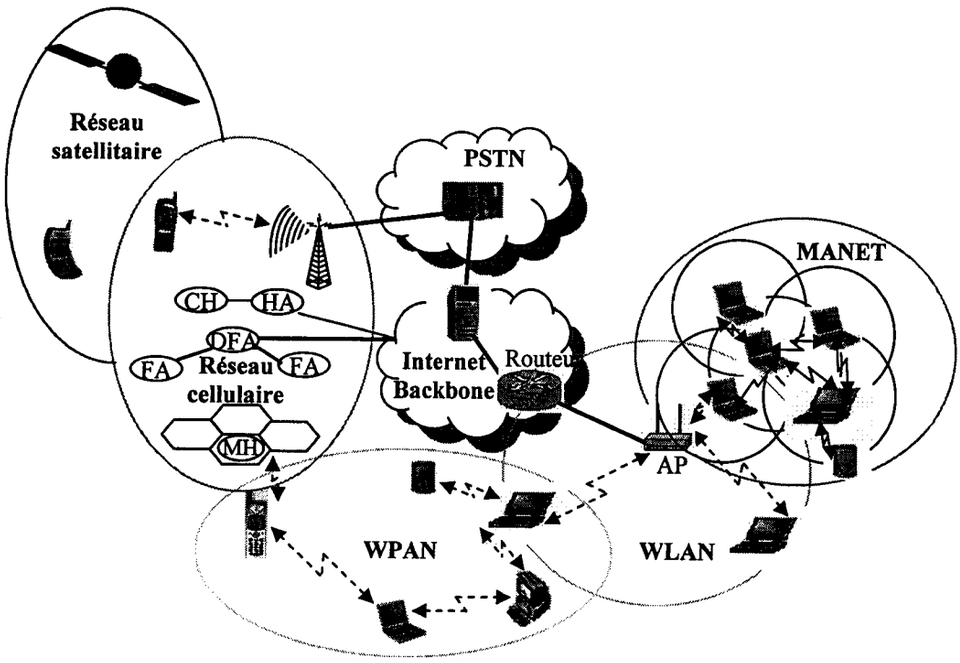


Figure I.6 : Réseaux 4G

Il existe deux niveaux d'intégration : l'intégration des différents types de réseaux sans fil hétérogènes avec leurs techniques de transmission (WLAN, WWAN, WPAN et les réseaux Ad hoc) ; et l'intégration des réseaux sans fil avec l'infrastructure fixe, l'Internet et le réseau téléphonique fixe. Cependant, beaucoup de travail reste à faire, pour permettre une intégration sans couture, comme par exemple l'extension du protocole IP (Internet Protocol) sur le support des stations mobiles.

I.7. Technologies et techniques de transmission dans les réseaux Ad hoc

Différentes techniques de transmission sont, ou peuvent être, utilisées dans les réseaux Ad hoc.

I.7.1. La couche physique

Deux différents médias peuvent être utilisés pour communiquer dans un réseau Ad hoc : les infrarouges et les radiofréquences.

- ***Infrarouge***

Les systèmes infrarouges sont simples, peu réglementés et peu coûteux. Ce médium convient aux réseaux à faible portée. Les émetteurs et récepteurs à infrarouge sont capables de fournir des débits très élevés à des coûts relativement faibles. De plus, les bandes passantes disponibles sont très larges et non réglementées. Les infrarouges pénètrent à travers le verre, mais pas à travers les murs ou

tout obstacle opaque, donc les communications se font dans une visibilité directe ; ceci facilite la sécurité. Il existe deux types de faisceaux infrarouges :

❖ ***Directifs :*** ils autorisent des débits plus élevés. Ces faisceaux nécessitent que l'émetteur et le récepteur soient en vue directe. La portée d'un tel système peut atteindre quelques kilomètres avec un débit de plusieurs dizaines de mégabit par seconde.

❖ ***Diffusants :*** ils ont une portée et un débit limités. Par contre, leur utilisation est relativement simple puisque les faisceaux peuvent se réfléchir sur les murs.

- ***Radiofréquence***

Le principe est d'émettre des ondes électromagnétiques qui constituent la porteuse du signal à transmettre. Le spectre radio est découpé en bandes de fréquences divisées en canaux. Aujourd'hui, on peut utiliser les bandes ISM pour les réseaux sans fil ; ces bandes sont gratuites, mais avec des contraintes d'utilisation (en temps et en puissance d'émission).

Afin de limiter la puissance d'émission tout en ayant un débit efficace, des techniques, appelées étalement de spectre, sont obligatoires dans certaines bandes (cas de la bande 2,4 GHz). Ces bandes ISM comportent les fréquences 868-870 MHz en Europe, 902-928 MHz en Amérique du nord, 2,4-2,4853 GHz et 5,725-5,85 GHz dans le monde. Ces fréquences sont reconnues par les organismes réglementaires internationaux pour une utilisation sans licence.

Il existe deux techniques classiques pour réaliser de l'étalement de spectre : DSSS et FHSS. Ces techniques ont donné leurs limites en termes de bande passante, c'est pourquoi on commence à voir, de plus en plus, une nouvelle technique qu'est l'UWB. Cette dernière est à l'étude dans plusieurs standards (IEEE 802.15.3a. et IEEE 802.15.4a).

- ***DSSS (Direct Sequence Spread Spectrum)***

En modulation par séquence directe, la porteuse est successivement modulée par l'information et par un code pseudo aléatoire. Le code pseudo aléatoire a une fréquence de modulation plus importante que l'information principale. Le signal résultant occupe donc une bande plus importante que la bande d'occupation en fréquence du message initial. Dans le récepteur, le signal reçu est multiplié par le code pseudo aléatoire pour récupérer l'information initiale. Cette technique présente les avantages suivants :

✓ La densité spectrale du signal transmis est faible car le signal est large bande ;

✓ Le signal étalé est moins sensible face à des signaux à bande étroite ;

✓ La tolérance vis à vis du multi-trajet est obtenue en choisissant des codes qui ont des facteurs d'auto corrélation très faibles.

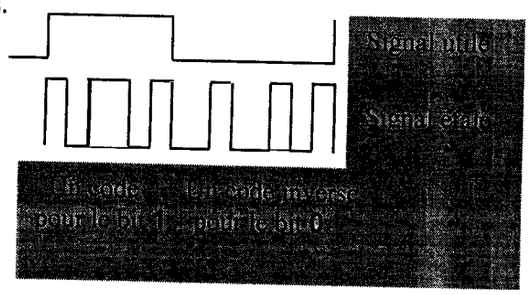


Figure I.7 : Etalement de spectre par séquence directe.

- ***FHSS (Frequency Hopping Spread Spectrum)***

Cette technique consiste à partager la bande passante en plusieurs sous-canaux. Le signal transmis saute de sous-canal en sous-canal (figure I.8) suivant une séquence de saut prédéterminée et généralement périodique. La séquence de saut de fréquence doit évidemment être synchronisée entre l'émetteur et le récepteur.

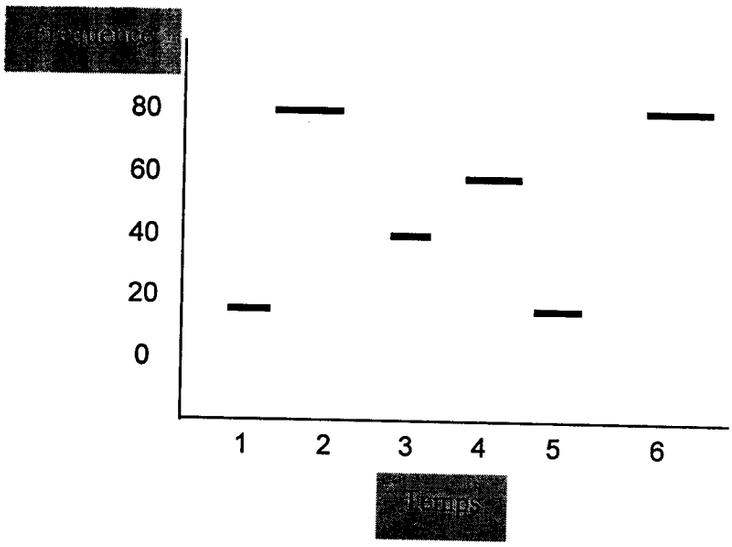


Figure I.8 : Etalement de spectre par saut de fréquence

Dans cette technique, le signal utile, ou l'information, est donc modulé en utilisant une modulation à bande étroite classique. Ensuite, la porteuse est décalée à un emplacement de la bande disponible en utilisant une séquence de fréquences pseudo aléatoire. Sur une longue durée, le signal obtenu est large bande.

- ***UWB (Ultra Wide Band)***

La notion de système ultra large bande UWB, n'est pas toujours clairement définie pour les systèmes de télécommunication. La terminologie UWB vient de la communauté du RADAR et désigne au départ des formes d'onde sans porteuses (carrier-free) faites d'impulsions de durée très courte (ordre de nano-seconde). Dans ce contexte, une définition communément admise est que ces signaux ont un rapport, largeur de bande sur fréquence centrale ou Fractional Bandwidth (FB)(équation I.1), supérieur ou égal à 0,20 et une largeur de bande supérieure à 500 MHz.

$$FB = 2\frac{f_H - f_L}{f_H + f_L} \qquad \text{(I.1)}$$

Où f_H et f_L sont les fréquences supérieures et inférieures à -3 dB.

Plusieurs standards, en cours de normalisation, s'appuient sur l'UWB car elle présente des caractéristiques intrinsèques très avantageuses. En effet, l'UWB donne déjà des débits très supérieurs à ceux donnés par les techniques de transmissions classiques. De plus, cette technique permet de faire de la géolocalisation qui peut être très utile dans un contexte de réseau Ad hoc.

I.7.2. La couche MAC (Medium Access Control)

Les caractéristiques principales de la sous couche MAC sont : le format des paquets, les techniques d'accès au médium, et la gestion du réseau. Les techniques d'accès au medium permettent à plusieurs utilisateurs de se partager les ressources. Ces techniques peuvent être classées en deux grandes familles, l'accès centralisé, où le réseau dispose d'une ou plusieurs stations de base qui gèrent l'allocation des canaux, et l'accès distribué où le réseau ne dispose pas de stations qui gèrent l'accès au canal.

- ***Accès centralisé***
  - ❖ ***FDMA (Frequency Division Multiple Access)***

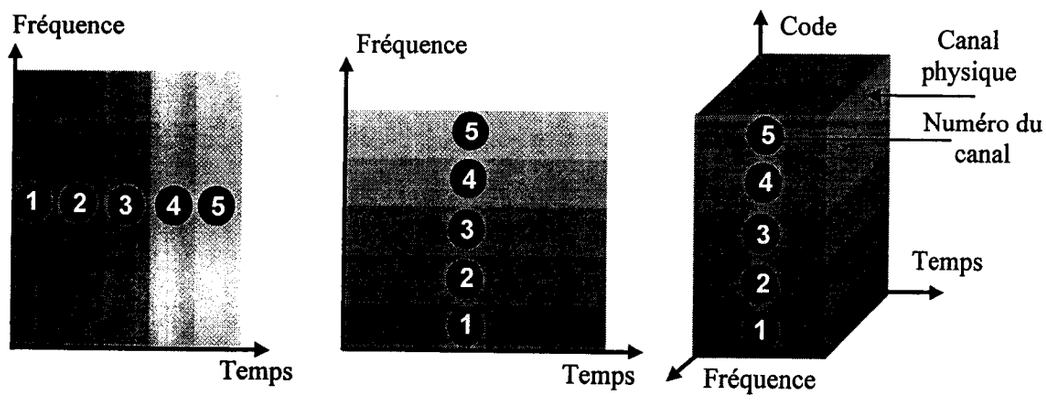
Le spectre est divisé en canaux. Chaque canal fréquentiel est affecté à un seul utilisateur à la fois. La méthode d'affectation est alors basée sur une règle de type premier arrivé, premier servi.

  - ❖ ***TDMA (Time Division Multiple Access)***

Les canaux sont multiplexés sous la forme d'intervalles de temps de telle manière que chaque utilisateur accède à toute la bande passante allouée pour le système de transmission durant un intervalle.

  - ❖ ***CDMA (Code Division Multiple Access)***

Chaque utilisateur émet sur un spectre étalé, obtenu au moyen d'un code pseudo aléatoire personnel. Ainsi tous les utilisateurs utilisent simultanément la même bande de fréquences. Ceci permet d'avoir une bonne immunité au bruit, d'utiliser la diversité de fréquences et le cryptage. Cette technique est très souple au niveau des débits transmis, mais relativement complexe car elle peut nécessiter une égalisation sur le récepteur et un contrôle de la puissance d'émission. Les techniques CDMA utilisent des modulations à étalement de spectre qui peuvent être réalisées par saut de fréquence ou par séquence directe.



a) FDMA *b) TDMA* *c) CDMA*

Figure I.9 : Accès centralisé

- ***Accès distribué***
  - ❖ ***ALOHA***

ALOHA est une technique d'accès utilisée au départ par l'université d'Hawaï, pour relier les centres informatiques dispersés sur plusieurs îles. Cette technique est le plus souvent utilisée dans les

réseaux satellitaires vu son faible taux d'accès au canal qui avoisine les 20%. Son principe est le suivant : les stations émettent, de façon inconditionnelle, des paquets dès qu'ils sont en leur possession, il n'y a pas d'écoute du support avant la transmission. Dans le cas d'une collision, la station va retransmettre les paquets après un délai aléatoire comme dans le cas du CSMA/CA introduit ci dessous.

❖ ***CSMA/CA (Carrier Sense Multiple Access - Collision Avoidance)***

Le principe de base du CSMA/CA est d'écouter avant d'émettre puis de tenter d'obtenir l'accès : si le lien est inoccupé lorsqu'une station cherche à transmettre des données, celle-ci envoie ses paquets. Si le canal est occupé, la station attend la fin de sa temporisation pour gagner le droit d'accès au medium. Lorsque sa temporisation expire, si le canal est inoccupé, la station envoie ses paquets. La station qui a obtenu aléatoirement la temporisation la plus courte est donc celle qui gagne le droit d'accès au médium. Les autres attendent alors simplement la fin de la transmission pour avoir le droit de tenter à nouveau l'accès au médium.

I.7.3. La couche MAC et spécifications liées aux réseaux Ad hoc

En l'absence d'infrastructure, les nœuds d'un réseau Ad hoc, les réseaux fortement chargés en particulier, ont besoin d'un protocole spécifique de contrôle d'accès au médium qu'ils partagent. La couche MAC apparaît en effet comme un goulot d'étranglement à forte charge. Les difficultés proviennent principalement des variations du canal radio, des changements possibles de topologie dus à la mobilité des nœuds. A cela il faut ajouter que les communications entre terminaux peuvent être multi-sauts, c'est pour ces raisons que contrôler l'accès au médium s'inscrit parmi les champs les plus actifs des domaines de recherche sur les réseaux Ad hoc.

La couche MAC, dont le but de définir les règles de partage des ressources radio, est confrontée à quatre problèmes principaux [6]:

(i) Les antennes ne peuvent fonctionner qu'en mode semi-duplex, c'est-à-dire qu'elles ne sont pas capables de transmettre et recevoir au même moment ;

(ii) Les transmissions sont soumises à un canal radio fluctuant et éventuellement à une topologie de réseau variable ;

(iii) Les mécanismes d'écoute de porteuse sont fragilisés par le problème du terminal caché ;

(iv) La capacité peut être réduite à cause du problème du terminal exposé.

I.8. Exemples de réseaux fonctionnant en mode Ad hoc

Maintenant nous allons voir les différents standards qui peuvent fonctionner dans le mode Ad hoc. Ces standards rentrent dans la catégorie des réseaux privés sans fil.

I.8.1. WiFi (WLAN - IEEE 802.11)

Ce standard est très connu actuellement, il concerne deux types d'équipements : une station sans fil ; en général un PC (Personal computer) équipé d'une carte réseau sans fil, et un point d'accès. Le standard définit deux modes [7] : un mode avec infrastructure et un mode Ad hoc.

En mode infrastructure, le réseau sans fil est constitué au minimum avec un point d'accès connecté à l'infrastructure du réseau filaire et un ensemble de postes sans fil. Cette configuration est

baptisée Basic Service Set (BSS, ou ensemble de services de base). Un Extended Service Set (ESS, ou ensemble de services étendu) est un ensemble d'au moins deux BSS formant un seul sous réseau.

Le mode Ad hoc (également baptisé point à point, soit IBSS- Independant Basic Service Set-) représente simplement un ensemble de stations sans fil 802.11 qui communiquent directement entre elles sans point d'accès ni connexion à un réseau filaire.

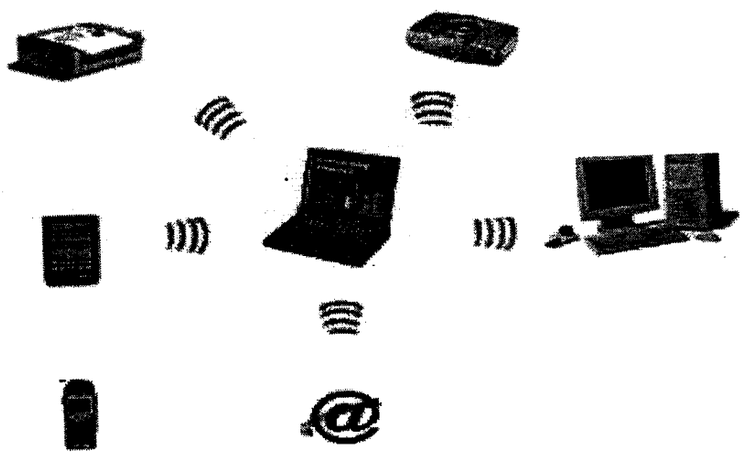


Figure I.11 : Exemple d'un réseau Bluetooth.

- ***Couche physique***

La couche physique Bluetooth utilise la bande de fréquence ISM à 2,4 GHz qui s'étale de 2400 à 2483,5 MHz et découpée en 79 canaux de 1 MHz. La modulation utilisée est la GFSK (Gaussian Frequency Shift Keying) avec un débit de 1 Mbit/s sur la voie radio.

Trois classes de puissance ont été définies : 100 mW (portée d'environ 100 mètres), 2,5 mW et 1 mW. Les récepteurs Bluetooth doivent quant à eux avoir une sensibilité au moins égale à -70 dBm.

La couche physique utilise l'étalement de spectre par saut de fréquences FHSS. Chaque paquet à transmettre est émis sur une fréquence différente de celle utilisée précédemment (1600 sauts par seconde). La séquence de saut est pseudo-aléatoire. Deux réseaux distincts n'ont pas la même séquence de sauts et ne sont pas synchronisés.

- ***Sous couche MAC***

Bluetooth a inauguré le concept de piconet : réseau éphémère se créant au gré des besoins. La gestion du piconet est centralisée et confiée à une station appelée maître. Par extension, toutes les stations non-maîtres incluses dans un piconet sont appelées esclaves comme montrés sur la figure I.11.

Ce sont les caractéristiques du maître qui définissent celles du piconet. En particulier chaque station Bluetooth possède une adresse (48 bits) ainsi qu'une horloge interne. La séquence de sauts pseudo-aléatoire qui définit le canal est initialisé en utilisant l'adresse du maître. Le maître gère également l'accès au piconet en attribuant à chaque nouvelle station une adresse courte sur 3 bits permettant à la station de communiquer au sein du piconet. La taille de l'adresse limite à 7 le nombre maximum d'esclaves actifs par piconet. L'adresse '000' est réservée au maître. Cette limitation peut en partie être levée grâce à l'interconnexion de plusieurs piconets par des stations charnières. L'ensemble constitué d'au moins deux piconets interconnectés est appelé scatternet.

I.8.3. HighRate (HR-WPAN, IEEE 802.15.3)

Développé au sein de l'IEEE, le standard HR-WPAN adopte une architecture tout à fait classique. Comme l'ensemble des standards de communication de la famille 802, le standard spécifie une sous couche MAC supportée par une couche physique (PHY).

Comme pour Bluetooth, le modèle de réseau Ad hoc avec une gestion centralisée par un maître a été adopté. Le maître est appelé ici PNC (PicoNet Coordinator). Il endosse toutes les responsabilités liées au piconet. Un PNC peut avoir jusqu'à 253 stations actives connectées à son piconet.

- ***Couche physique***

La couche physique de ce standard utilise la bande ISM à 2,4 GHz. La modulation QPSK est utilisée pour le mode de base avec un débit de 11 Mbit/s. Quatre autres modulations sont également définies : DQPSK (Differential QPSK), 16 QAM, 32 QAM et 64 QAM fournissant des débits respectifs de 22, 33, 44 et 55 Mbit/s.

La bande ISM a été divisée en quatre canaux de 15 MHz. Un mode compatible 802.11b n'utilisant que trois canaux et destiné à améliorer la coexistence entre les systèmes 802.15.3 et 802.11b est également disponible. Les sensibilités sont spécifiées pour chaque type de modulation, la plus petite est celle de la modulation QPSK et qui est de -82 dBm pour la modulation.

Cependant, cette couche physique n'intéresse plus maintenant les industriels. En effet, l'avènement de l'UWB a changé la donne et a poussé donc la création du groupe 802.15.3a qui opte pour une couche physique UWB et fournie des débits allant jusqu'à 480 Mbit/s.

- ***Sous couche MAC***

Le canal de transmission est divisé temporellement en supertrames. Chaque supertrame se décompose en trois parties : une trame balise (Beacon), la CAP (Contention Access Period) et la CFP (Contention Free Period).

La supertrame a une durée paramétrée par le PNC pour répondre aux besoins des participants du piconet. La trame balise, la CAP et la CFP peuvent elles aussi avoir des tailles variables d'une supertrame à l'autre. La taille de la trame balise est fonction des informations à transmettre. Cette trame est transmise par le PNC au début de chaque supertrame. Elle est destinée à l'ensemble des stations pour informer des paramètres du piconet. Parmi ces paramètres on trouve la durée de la supertrame, de la CFP mais aussi des informations d'allocations de ressources.

La durée de la CFP est fonction des besoins des stations en ressource. Plus les demandes sont importantes, plus la part de la CFP dans la supertrame est importante. Le temps restant est alloué à la CAP.

La CAP n'est utilisé que pour la transmission des trames de commandes et de certaines trames de données lorsque l'expéditeur ne possède pas de ressources déjà allouées dans la CFP. L'accès au canal pendant la CAP se fait avec du CSMA/CA simplifiés par rapport à celui présents dans la sous couche MAC du standard 802.11.

I.8.4. ZigBee (LR-WPAN, IEEE 802.15.4)

Le comité IEEE a terminé de normaliser le standard 802.15.4 (Low Rate WPAN). Les objectifs principaux de cette nouvelle norme, concurrente à la technologie Bluetooth dans certaines applications, sont de mettre au point une technologie qui permet un transfert fiable de données, une installation facile, un bas coût et une très basse consommation.

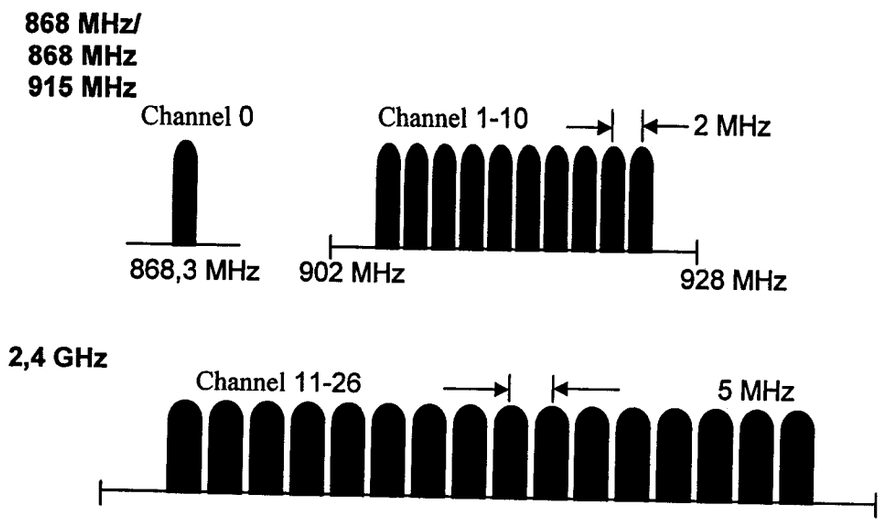


Figure I.12 : Bande de fréquence de l'IEEE 802.15.4.

Les applications ciblées peuvent être : le contrôle médical (biotélémétrie), la logistique (contrôle des marchandises dans un entrepôt, grandes surfaces), le contrôle industriel (réseaux de capteurs), la domotique (jouets, commande de périphériques), etc.

- ***Couche physique***

Au niveau de la couche physique, la norme 802.15.4 offre deux options qui, combinées avec la sous couche MAC, permettront la mise en œuvre d'une large gamme d'applications. Les deux couches physiques sont basées sur les techniques d'étalement de spectre par séquence directe (DSSS). La première couche physique opère dans la bande 2,4 GHz et offre un débit de 250 kbit/s avec une modulation du type OQPSK (Offset QPSK). La seconde opère dans les bandes 868/915 MHz et offre un débit de 20 kbit/s pour la bande 868 MHz et 40 kbit/s pour la bande 915 MHz, la modulation utilisée ici est la BPSK.

Ce standard définit 27 canaux de transmission, 16 canaux dans la bande 2,4 GHz, 10 canaux dans la bande 915 MHz et 1 canal dans la bande 868 MHz (figure I.12).

- ***Sous couche MAC***

L'IEEE 802.15.4 peut fonctionner en deux modes. Dans le premier mode (avec supertrames), une station, appelée coordinateur du réseau, transmet des balises dans des intervalles prédéterminés. La durée de ces intervalles peut varier de 15 ms à 245 s. Le temps entre deux balises est divisé en 16 slots égaux. Un dispositif peut transmettre uniquement au début des slots. L'accès aux canaux est basé sur la méthode CSMA/CA; cependant, le coordinateur de réseau peut assigner des slots de temps à un dispositif exigeant des transmissions fiables ou celles dont le temps de latence est réduit. Ces slots réservés s'appellent des GTS (Guaranteed Time Slot) et forment un ensemble de slots situés dans la CFP.

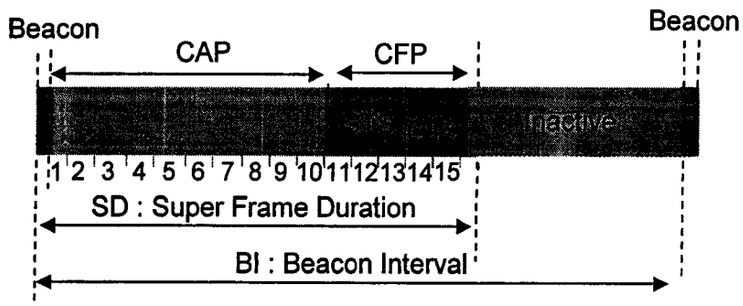


Figure I.13 : Structure de la supertrame IEEE 802.15.4.

Dans le second mode, le coordinateur de réseau n'envoie aucune balise. Dans ce cas, l'accès au médium se fait par la méthode d'accès CSMA/CA classique. Comme dans la plupart des communications sans fil, des trames d'acquittement peuvent être utilisées dans les deux modes.

I.9.Modèles de mobilité et contrôle de topologie dans les réseaux Ad hoc

I.9.1. Modèles de mobilité

En raison de la mobilité inhérente dans l'environnement Ad hoc, les performances des applications sont fortement influencées. La gestion de telle mobilité relève du défi, la recherche des moyens de modélisation sera donc une nécessité immédiate.

Les modèles de mobilité peuvent être regroupés en deux familles principales : les modèles de mobilité d'entité, et ceux de mobilité de groupe. Dans la première, les mouvements des noeuds mobiles (MNs) sont indépendant l'un de l'autre, alors que dans la deuxième, les décisions sur le mouvement dépendent des autres noeuds mobiles appartenant au même groupe. Après l'étude et l'analyse des divers modèles de mobilité, Camp et al.ont montré que :

- Les performances d'un protocole de réseau Ad hoc peuvent changer de manière significative selon le modèle de mobilité utilisé;
- Les performances d'un protocole de réseau Ad hoc peuvent changer de manière significative quand le même modèle de mobilité est employé avec différents paramètres;
- Les performances d'un protocole de réseau Ad hoc devraient être évaluées avec le modèle de mobilité qui assortit le plus étroitement le scénario réel prévu.

I.9.1.1. Modèles de Mobilité d'entité [8]

- *Random Walk Mobility* : développé par Zonoozi et Dassanayake, c'est un simple modèle de mobilité, dans lequel un noeud mobile se déplace de son emplacement courant vers un autre en effectuant des choix aléatoires pour la direction ainsi que la vitesse de déplacement. Les nouveaux paramètres (direction et vitesse de déplacement) sont choisis dans un ordre de grandeur prédéfini, [vitesse$_{min}$, vitesse $_{max}$] et [$0, 2\pi$] respectivement. □
- *Random Waypoint Mobility Model (RWP) :* défini par Johnson et Maltz. Pour ce modèle, tous les nœuds sont uniformément distribués autour de l'espace modelé (simulé) et les noeuds ont des périodes de pause et des périodes de mouvement. Un noeud mobile reste dans un endroit pendant un temps de pause fixe, puis il choisit une destination aléatoire et se déplace vers cette destination avec une vitesse uniformément distribuée dans l'intervalle [0, vitesse $_{max}$]. Pour atteindre la destination choisie, le noeud

fait une pause, et puis répète le processus le long du temps de simulation. Ce modèle est sans mémoire c-àd les endroits courants sont indépendants des précédents. Malheureusement, la simplicité de ce modèle n'est pas toujours adaptée pour décrire le comportement complexe de mobilité des utilisateurs.

• *Random Direction Mobility Model* : développé par Royer el al, Il apparaît comme une modification du modèle de RWP. Dans RWP, pour un noeud mobile, la probabilité de choisir une nouvelle destination située au centre du secteur de simulation (modélisation) ou se déplaçant par le centre est haute. Ce modèle essaye d'alléger ce comportement, en fournissant un nombre semi-constant de voisins dans tout l'espace de la simulation. Les noeuds mobiles choisissent une direction aléatoire comme dans le cas du modèle RWP, donc ils se déplacent vers la frontière de la simulation dans cette direction. Une fois que la frontière est atteinte, le noeud mobile fait une pause pendant le temps spécifié, choisit une autre direction angulaire entre (0 et 180)° et continue alors le processus.

• *Brownian Motion Model* : c'est un modèle complètement aléatoire. La direction du mouvement est une variable aléatoire continue entre 0 et 2π, la vitesse est aussi aléatoire à tout moment. Chaque nœud mobile se déplace dans une certaine surface après une période aléatoire, dont le mouvement est complètement isolé.

• *Manhattan Grid Model* : dans ce modèle chaque nœud mobile commence d'un point aléatoire situé dans une certaine rue"street", ensuite il fait le choix d'une destination aléatoire vers laquelle il se déplace avec une vitesse prédéfinie. Durant sa recherche de la destination, le nœud fait des temps de pause avant de répéter le processus. Il est supposé que le nœud se déplace, uniquement, verticalement ou horizontalement.

I.9.1.2. Modèles de Mobilité de groupe

• *Column Mobility Model* [8] : c'est un modèle de mobilité de groupe dans lequel un ensemble de nœuds mobiles forme une ligne ou une colonne, et se déplacent uniformément suivant une direction particulière. Initialement, chacun a un point de référence, de telle façon que tous les points forment une ligne. Individuellement, les nœuds mobiles ont la possibilité de se déplacer de façon aléatoire autour de leurs points de référence en utilisant un modèle de mobilité d'entité.

• *Nomadic Community Mobility* [8] : développé par Sanchez, représente un groupe de nœuds mobiles qui se déplacent ensemble d'un point vers un autre. Au sein de chaque groupe, le nœud mobile maintient sa propre région dans laquelle il effectue des mouvements aléatoires. La visite d'un musée par un groupe de touristes représente un bon exemple de ce modèle, ces touristes se déplacent ensemble pour visiter le musée, dont chaque touriste peut rejoindre une location particulière.

• *Pursue Model (PM)* [8] : défini par Sanchez, il essaye de représenter des noeuds mobiles dépistant une cible spécifique appelée ' leader '. Ce genre de comportement est trouvé dans des activités multiples de robots. Un noeud particulier dans chaque groupe agit en tant que 'leader ', et il se déplace selon un modèle de mobilité d'entité, généralement, le modèle de RWP, les noeuds restants dans le groupe se déplacent vers le 'leader'. Ces noeuds, appelés nœuds de poursuite, choisissent une vitesse aléatoire uniforme dans la gamme $[V_{min}, V_{max}]$. La vitesse des noeuds ne change pas avec le déplacement. La prochaine position de chaque noeud mobile est calculée en fonction de la position

courante, d'un vecteur aléatoire et d'une fonction d'accélération, en utilisant une équation simple de mise à jour :

New_Position=Old_Position + acceleration (target – Old_Position) + Random_Vector (I.2)

• *Reference Point Group Mobility Model (RPGM)* [8] : défini par Hong, Gerla et al. Il propose un mouvement aléatoire d'un groupe de noeuds mobiles ainsi qu'un mouvement aléatoire de chaque noeud mobile appartenant à ce groupe. Chaque groupe a son propre comportement de mobilité. Il y a " centre " logique pour chaque groupe, tel que le mouvement de ce 'centre' définit le mouvement du groupe entier (position, vitesse, direction et accélération), en suivant le modèle de RWP, chaque nœud du groupe suit ce centre logique. Le mouvement des groupes est explicitement défini en donnant un chemin de mouvement pour le centre. Les différents noeuds mobiles appartenant à un groupe se déplacent aléatoirement autour de leurs propres points de référence prédéfinis, dont les mouvements dépendent du mouvement de groupe.

I.9.2. Contrôle de topologie dans les réseaux Ad hoc

La topologie du réseau joue un rôle déterminant dans le fonctionnement des protocoles de contrôle utilisés, sur la capacité ainsi que sur les performances du réseau d'une manière générale. Le contrôle de topologie dans les réseaux Ad hoc est un domaine de recherche récent. Il vise à maintenir une topologie adéquate en maîtrisant les liens à inclure dans le réseau. Le but est d'atteindre un ensemble d'objectifs comme : réduire les interférences, réduire la consommation d'énergie, ou augmenter la capacité du réseau.

Vu les capacités limitées des équipements mobiles en terme d'énergie, les premiers travaux pour le contrôle de topologie dans les réseaux Ad hoc utilisent la consommation d'énergie comme métrique, et sont basés sur l'ajustement de la puissance de transmission des noeuds. Ces techniques de contrôle peuvent être centralisées ou distribuées. Dans les algorithmes de contrôle de topologie centralisés, une entité centrale calcule la puissance de transmission en utilisant la position des noeuds du réseau afin de réaliser une topologie avec une forte connectivité. Dans les algorithmes distribués, les noeuds mobiles ajustent leur puissance de transmission selon des informations locales pour maintenir un nombre fini de voisins.

Une autre approche pour contrôler la topologie du réseau Ad hoc est basée sur l'utilisation d'un sous-ensemble de noeuds du réseau pour servir de 'Cluster Head' (super noeud) doté de fonctionnalités additionnelles. Cette approche, souvent appelée 'Cluster Based Protocol', qui consiste à élire un ensemble de cluster-heads, où chaque noeud mobile est associé à un cluster-head. L'élection permet de réduire la maintenance de la topologie dans les réseaux Ad hoc. Cependant, elle a un impact négatif sur les cluster-heads, parce que ces derniers consomment leur énergie plus rapidement qu'un noeud classique. Une solution est de considérer l'équilibrage des charges dans l'algorithme d'élection. Le but d'une telle approche est de réduire la surcharge additionnelle du réseau et complexité de la maintenance, et de simplifier des fonctions essentielles comme : le routage, le contrôle de puissance, la sécurité, . . . etc.

I.10. Difficulté du routage dans les réseaux Ad hoc et inadaptation des techniques conventionnelles

Le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Le problème de routage, consiste pour un réseau dont les arcs, les nœuds et les capacités sur les arcs sont fixés, à déterminer un acheminement optimal des paquets (de messages, de produits ...etc.) à travers le réseau pour certains critères de performance (bande passante, délai, etc.). Il doit aussi être de capable de s'adapter aux événements venant perturber le réseau (panne, congestion, ...etc.).

Les protocoles classiques adoptés et qui ont prouvés leurs fiabilités, ont été conçus pour des réseaux filaires ayant des topologies statiques, et sont exécutés par des noeuds dotés de suffisamment de ressources.

Les protocoles de routage dans les réseaux Ad hoc opèrent dans des réseaux dont les changements de topologie sont fréquents, et sont exécutés sur des équipements, pouvant être hétérogènes, ayant des contraintes de ressources (de batterie, de mémoire, de CPU, etc.), ces caractéristiques rendent alors l'utilisation des protocoles filaires classiques inadéquate.

Des expérimentations ont été menées à l'Irisa (Rennes) [9] pour montrer l'inefficacité d'IP pour les réseaux mobiles. Les résultats obtenus montrent que l'échange des tables de routage occupent plus de 90 % de la bande passante et présentent des défauts de mise à jour lors de modifications de topologie trop fréquentes.

En plus, TCP (Transmission Control Protocol) est un protocole de transfert qui garantit une livraison fiable et ordonnée des paquets de données sur un réseau filaire. Malgré son bon fonctionnement sur ces réseaux, le TCP performe très mal sur les réseaux mobiles Ad hoc. C'est dû à ce que la supposition implicite de TCP affirmant que toute perte de paquet est causée par la congestion est invalide dans les réseaux mobiles Ad hoc, où les pertes et les erreurs sont causés par le canal sans fil, le partage du lien entre plusieurs usagers, ainsi que le routage multi trajet et la mobilité. Si le TCP interprète de telles pertes comme étant de la congestion et qu'il appelle alors des procédures de contrôle de la congestion, le réseau souffrira d'une dégradation de performances.

Pour pallier à ce type de problème, la conception des stratégies de routages doit tenir compte de tous les facteurs et limitations physiques imposés par ces réseaux, afin que les protocoles de routage résultants ne dégradent pas les performances du système.

Ces dernières années, plusieurs protocoles de routage Ad hoc ont été proposés, soit en modifiant les protocoles de routage conventionnels, soit en élaborant de nouvelles approches de routage. Ces protocoles peuvent être classés, suivant les critères de classification, en plusieurs familles. Selon la classification, la plus connue, qui utilise la manière de création et de maintenance des routes, lors de l'acheminement des données, ces protocoles son classés en trois catégories. Les protocoles proactifs et les protocoles réactifs, et une troisième dite hybride mixe ces deux premières. Ces différents protocoles seront présentés dans le chapitre deux.

I.11. La qualité de service dans les réseaux Ad hoc

Le RFC 2386 caractérise la QoS (Quality of Service) comme un ensemble de besoins à assurer par le réseau pour le transport d'un trafic d'une source à une destination. Suivant le type de l'application, les besoins de QoS sont différents. Par exemple, pour les applications temps réel, comme la voix et la vidéo, le délai de bout en bout d'un paquet doit être limité, autrement le paquet est inutile. Les applications non temps réel, comme le transfert de fichier ou la messagerie, quant à elles se focalisent sur la fiabilité des communications.

Le support de la qualité de service a été largement étudié dans les réseaux filaires. Des solutions ont été proposées afin de fournir la QoS aux communications multimédia et des mécanismes ont été fournis pour gérer efficacement les ressources réseau (bande passante, mémoire tampons) pour répondre aux exigences de ces applications.

Suite à la grande variété des applications des réseaux Ad hoc, la qualité de service dans ces réseaux est devenue un thème de recherche qui a suscité beaucoup d'intérêt.

Wu et Harms introduisirent une classification des approches proposées [3].Cette classification regroupe les propositions de solutions en quatre catégories : premièrement les modèles de qualité de service regroupant des définitions d'architectures destinées à assurer cette dernière, deuxièmement les protocoles de signalisation définissant un ensemble de paquets de contrôle, destinés par exemple à provoquer la réservation de ressources dans les routeurs. Troisièmement les protocoles de routage avec qualité de service qui se chargent de la recherche de routes répondant à certains critères. Enfin, les protocoles d'accès au médium avec qualité de service fournissant un ensemble d'outils permettant de mettre en œuvre certaines règles de qualité de service.

Cependant, il est très difficile de garantir une quelconque qualité de service à une application temps réel dans un réseau Ad hoc, pour les raisons citées précédemment

I.12. La sécurité dans les réseaux Ad hoc

La sécurité est un problème majeur à traiter, puisque cette nouvelle génération de réseaux engendre de nouvelles contraintes et de nouveaux problèmes, liés à leur spécifications, pour la sécurité tels que : la sécurité du routage, la mise en œuvre de mécanismes de sécurité non centralisés.

Ainsi, les noeuds sont exposés au vol car ils sont mobiles et la capacité de calcul est limitée, ce qui fait que l'utilisation de solutions lourdes comme les PKI, n'est pas pratique ici. Aussi, les services dans les réseaux Ad hoc sont provisoires et les batteries sont une source limitée d'énergie. Cette dernière vulnérabilité fait que les attaques par Dénie de Service [10] et par consommation d'énergie sont possibles.

Plusieurs approches et solutions ont été proposées pour sécuriser les réseaux Ad hoc. Chacune se base sur un raisonnement différent suivant le type d'application, l'extension du réseau , la moyenne du nombre de noeuds ainsi que les aspects de sécurité pris en priorité (confidentialité, authenticité,...) . On trouve par exemple l'IPsec (IP security), le WEP (Wireless Equivalent Privacy), le modèle de confiance distribué, l'accord à clé basé sur un mot de passe (key agreement based password), la politique de sécurité (Resurrecting Duckling), la cryptographie à seuil, et ou la sécurité du routage

SRP(*Secure Routing Protocol)*. Il n'y a pas de solution globale pour tous les types de réseaux Ad hoc, et aucune n'est assez résistante pour toutes les vulnérabilités. Il y a juste, des solutions pour des problèmes spécifiques.

I.13. Conclusion

Après avoir défini l'environnement mobile Ad hoc et décrit ses principales caractéristiques, les avantages et les inconvénients qu'il présente et les différents domaines d'applications qui ont recours à ce type de réseaux sans fil. Nous avons présenté dans ce chapitre quelques exemples de réseaux qui peuvent fonctionner en mode Ad hoc, les spécifications que doit avoir la couche MAC, les modèles proposés pour la modélisation et gestion de la mobilité, le contrôle de la topologie qui vise à maintenir une topologie adéquate puisque cette dernière joue un rôle déterminant dans le fonctionnement des protocoles de contrôle utilisés.

Nous avons parlé aussi du problème de routage dont les techniques classiques utilisées dans les réseaux filaires sont mal adaptées. Une grande partie des travaux dans les réseaux Ad hoc se sont concentrés sur la problématique du routage, l'avancée de ces travaux a permis de proposer plusieurs approches. L'étude de ce problème, et les différentes solutions proposées fait l'objet du chapitre suivant.

Chapitre II

Le routage dans les réseaux Ad hoc

II.1. Introduction

Comme nous l'avons déjà vu, un réseau Ad hoc est un ensemble de nœuds mobiles qui sont dynamiquement et arbitrairement éparpillés et où l'interconnexion entre les nœuds peut changer à tout moment. Dans la plupart des cas, la station de destination ne se trouve pas obligatoirement à la portée de la station émettrice, ce qui nécessite l'emploi d'un routage interne via des stations intermédiaires. L'intérêt du routage consiste à trouver le chemin optimal au sens qu'il doit vérifier un certain nombre de critères de performances (bande passante, débit, délai,...).

La topologie dynamique et le peu de ressources (bande passante, énergie...), rendent difficile la conception des stratégies de routage. Cependant, ces dernières années plusieurs protocoles de routage Ad hoc ont été proposés, soit en modifiant les protocoles de routage classiques, soit en élaborant de nouvelles approches. Le but de ce chapitre est de donner un état de l'art des solutions proposées. Nous allons présenter un bref rappel des techniques classiques, puis la conception des stratégies de routage Ad hoc, la classification des protocoles résultants, ainsi que la description de quelques protocoles, et pour terminer nous donnerons les extensions apportées à ces protocoles pour améliorer la qualité de service, la sécurité et l'économie d'énergie.

II.2. Les techniques de routage conventionnelles

On distingue généralement deux familles d'algorithmes de routage :

- ***Le routage par état des liens (Link State)***

Ils cherchent à maintenir dans chaque noeud une carte plus ou moins complète du réseau où figurent les noeuds et les liens. A partir de cette carte, il est possible de construire les tables de routage. Un des avantages de ce type de protocole est leur capacité à pouvoir facilement trouver des routes alternatives lorsqu'un lien est rompu. Il est même possible d'utiliser simultanément plusieurs routes vers une même destination, augmentant ainsi la répartition de la charge et la tolérance aux pannes dans le réseau. En contre partie, si le réseau est étendu, la quantité d'information à stocker et à diffuser peut devenir considérable. Pour calculer les routes optimales vers un nœud, il sera facile d'utiliser l'algorithme de Dijkstra [11].

- ***Le routage par vecteur de distance (Distance Vector)***

Dans ce type de routage, un nœud échange avec ses voisins une estimation de la distance vers tous les nœuds du réseau. Cet échange d'information couplé avec un algorithme de recherche du plus

court chemin (Bellman, Ford et Fulkerson) [11] permet à chaque nœud de converger vers une connaissance exacte de la topologie du réseau. Il est possible de montrer que, dans le cas d'un réseau statique, l'algorithme converge vers la topologie exacte du réseau. Dans le cas de la perte d'un lien, l'algorithme peine à converger de nouveau vers la topologie exacte

On peut citer deux types différents de routage par vecteur de distance ou par état des liens:

- ***Le routage à la source (source routing)***

Le routage à la source consiste à marquer dans le paquet routé l'intégralité du chemin que va suivre le paquet pour atteindre sa destination. L'entête du paquet va donc contenir la liste des différents nœuds relayeurs vers la destination.

- ***Le routage saut par saut (hop by hop routing)***

Ce type de routage consiste à donner uniquement à un paquet l'adresse du prochain nœud, mais qui le mènera fatalement vers sa destination. Ce type de routage est le routage le plus répandu dans l'Internet, c'est le système de routage par défaut.

II.3. Limitation des techniques conventionnelles dans les réseaux Ad hoc

Dans les réseaux Ad hoc, on est presque sur de passer par plusieurs nœuds (multi-hops) avant d'atteindre la destination. Dans les solutions traditionnelles de routage, chaque noeud dans le réseau maintient une table de routage qui présente, pour chaque destination connue, le prochain noeud auquel un paquet devrait être envoyé. Le problème pour maintenir ces tables devient plus difficile dans les réseaux Ad hoc, suite aux fréquents changements de topologie.

Le défi dans la création d'un protocole de routage pour les réseaux Ad hoc est de concevoir un simple protocole qui peut s'adapter à la grande variété de conditions du réseau.

Dans les réseaux filaires, les protocoles de routage sont conçus pour une topologie statique, ils dépendent fortement des messages périodiques de contrôle. Ils exigent l'échange fréquent des tables d'état de lien ou des vecteurs de distance. Ce type de routage provoque la surcharge du canal et des coûts supplémentaires dans les réseaux Ad hoc. En outre, les algorithmes de vecteur de distance, comme le DBF (Distributed Bellman Ford) [8], sont peu performants dans les réseaux mobiles en raison de leur lente convergence.

Ainsi, les protocoles traditionnels consomment beaucoup de ressources telles que la largeur de bande, la puissance de batterie, et l'unité centrale de traitement (CPU), et par conséquent ils ne sont pas appropriés dans les réseaux Ad hoc .D'autre part, ils assument des liens bi-directionnels, ce qui n'est pas toujours le cas dans un environnement sans fil [8].

II.4. Définition du problème de routage dans les réseaux Ad hoc

Lorsqu'on joint par une branche les noeuds qui sont réciproquement dans la portée de leur interface radio on dessine un graphe (aléatoire) qui a une forme comme celle illustrée par la figure II.1. Le problème du routage revient, entre deux noeuds quelconques, à calculer le « meilleur » chemin qui permet de les joindre.

Il s'agit d'un problème de plus court chemin dans un graphe pour lequel existent plusieurs algorithmes performants (Ford-Bellman, Dijkstra, sont les plus connus), mais la vraie difficulté est

ailleurs. Chaque noeud doit avoir sa table de routage à jour, il faut donc maintenir ces tables (les noeuds sont mobiles, ils peuvent apparaître ou disparaître, leur activité varie dans le temps). Cette contrainte est la cause d'un overhead non négligeable dans le réseau, les mobiles doivent émettre des informations de mise à jour de ces tables. Cet overhead augmente avec la taille du réseau et la mobilité des noeuds. Les différents algorithmes de routage qui sont proposés (par exemple par l'IETF) ont pour objet la résolution de ce problème [4].

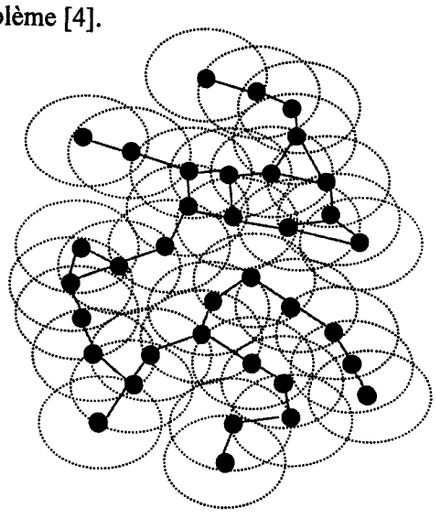


Figure II.1: maillage aléatoire

Il y a aussi une difficulté dans le choix du critère permettant de dire qu'une route est « meilleure » qu'une autre, cela dépend de la structure du réseau et de ses caractéristiques : la taille et la densité du réseau et vitesse de déplacement des nœuds, Il s'agit d'affecter une métrique « longueur » à chaque arête du graphe, de sorte que la longueur d'un chemin est la somme des longueurs des branches qui le constituent. Plusieurs métriques sont possibles, en particulier :

- Le nombre de branches du chemin;
- La qualité de chaque branche, afin de privilégier les liens de bonne qualité parce qu'on peut y faire passer plus d'information. De plus si un mécanisme de retransmission est prévu sur chaque lien, choisir un bon lien minimise le nombre de retransmissions et donc le retard de bout en bout. On peut aussi pondérer plusieurs métriques.

II.5. Conception des stratégies de routage dans les réseaux Ad hoc

Les protocoles de routage, destinés à ce genre de réseaux, doivent satisfaire les critères suivants [1-11] :

➢ ***Traitement distribué***

Un réseau Ad hoc ne doit dépendre d'aucune entité centralisée, contrairement aux réseaux câblés, et par conséquence l'algorithme de routage doit être un algorithme distribué ne nécessitant pas le recours à un nœud assurant une coordination de « chef d'orchestre » ;

➢ ***Absence de boucle***

Ceci pour éviter que des paquets tournent dans le réseau pendant un temps indéfini. Les solutions basées sur les valeurs de TTL (Time To Life) peuvent contrer ce problème, mais une approche plus structurée est préférable pour améliorer l'exécution globale;

➢ ***Traitement proactif ou sur demande***

Plutôt que de maintenir des tables de routage dans tous les nœuds tout le temps, l'algorithme de routage calcule la route à chaque demande de trafic, et en temps réel. Si ceci est fait intelligemment, on peut utiliser plus efficacement les ressources du réseau et de la bande passante, malgré le coût en temps dédié à la découverte de nouveaux itinéraires.

➢ ***Traitement des périodes de veille (sommeil)***

Pour conserver leur énergie ou parce qu'ils ont parfois besoin d'être inactifs, les nœuds d'un réseau Ad hoc peuvent s'arrêter de transmettre ou de recevoir pendant un certain temps. Un protocole de routage devrait être capable de supporter les périodes de veille et les utiliser pour conserver au maximum l'énergie au niveau des nœuds, sans qu'elles aient trop de conséquences défavorables sur le réseau ;

➢ ***Souplesse***

Il doit sauvegarder les différentes routes afin de réagir rapidement aux changements de la topologie et tout genre d'incident sur le bon acheminement des données (par exemple, l'élimination d'un lien, pour cause de panne ou pour cause de mobilité);

➢ ***Sécurité***

Sans une certaine forme de sécurité au niveau de la couche réseau ou physique, un protocole de routage Ad hoc est vulnérable à plusieurs types d'attaques. Il est sans doute assez facile d'écouter le trafic, de rejouer les transmissions, de manipuler les en-têtes de paquets ou de rediriger les messages de routage dans un réseau sans fil n'ayant pas de dispositions appropriées en termes de sécurité. Même si ces soucis existent déjà au sein des infrastructures câblées et des protocoles de routage, assurer une certaine sécurité "physique" des éléments de transmission est plus difficile en pratique avec les réseaux Ad hoc. Une protection suffisante pour empêcher le déni de service ou la modification des opérations du protocole est préférable. Celle-ci sera sans doute différente des autres approches pour la sécurité des protocoles de routage, comme les techniques de sécurité IP;

➢ ***Qualité de service***

Un réseau Ad hoc doit assurer une certaine forme de qualité de service qui dépend du domaine d'utilisation du réseau ;

➢ ***Support des liaisons unidirectionnelles***

Les liaisons sont généralement supposées bidirectionnelles lors de la conception des algorithmes de routage et beaucoup d'algorithmes ne fonctionnent pas normalement avec des liaisons unidirectionnelles. Néanmoins, les liaisons unidirectionnelles sont bien présentes dans les réseaux sans fil. La plupart du temps, un nombre suffisant de liaisons en duplex existent, ce qui fait des liaisons unidirectionnelles une valeur ajoutée, mais limitée. Pourtant, quand il y a une paire de liaisons unidirectionnelles (de directions opposées), cela peut créer la seule connexion bidirectionnelle entre deux régions Ad hoc. La possibilité de les utiliser devient alors très intéressante ;

➢ ***Délais de transmission de bout en bout***

Délais de transmission de bout en bout pour un trafic utilisant la fonctionnalité du routage. Ce délai est une variable aléatoire

➢ ***Temps d'acquisition d'itinéraires***

Une forme particulière de mesure externe des délais de bout en bout. Cette mesure a un intérêt particulier pour les algorithmes de routage « à la demande ».

➢ ***La minimisation de la charge du réseau***

L'optimisation des ressources du réseau renferme deux autres sous problèmes qui sont les boucles infinies de routage, et la concentration du trafic autour de certains nœuds ou liens.

II.6. L'évaluation des protocoles de routage

De même que le routage dans les réseaux filaires, il est peu probable qu'un protocole soit la meilleure approche dans tous les contextes des réseaux Ad hoc. Les paramètres qui définissent un contexte de réseau et qui devraient être considérés pendant la conception du protocole, la simulation et la comparaison incluent :

❖ ***Taille du réseau :*** mesurée en nombre de nœuds;

❖ ***Connectivité du réseau :*** en termes de nombre moyen des voisins d'un noeud;

❖ ***Taux de changement topologique :*** le taux avec lequel la topologie d'un réseau change;

❖ ***Capacité de lien :*** vitesse efficace de lien, mesurée en bits/seconde ;

❖ ***Fraction des liens continus :*** efficacité du protocole avec la présence des liens unidirectionnels ;

❖ ***Modèles de trafic :*** différents types de distribution du trafic éprouvés dans un réseau

❖ ***Mobilité :*** influence du changement topologique sur les performances d'un protocole de routage et le choix du modèle le plus approprié pour la mobilité des nœuds ;

❖ ***Fraction et fréquence des veilles des noeuds :*** performances du protocole en présence de périodes de veille.

La liste précédente donne une indication du nombre de paramètres qui devrait être considérés, dans l'évaluation des protocoles, pendant un processus de standardisation. Ces issues d'évaluation proclament les performances en fonction d'une métrique donnée, ce qui peut aider à favoriser des comparaisons et des évaluations significatives des performances du protocole. Ces issues différencient les réseaux Ad hoc des réseaux filaires.

Il devrait être connu qu'un protocole de routage tend à être bien adapté pour des contextes particuliers du réseau, et moins approprié pour d'autres. En mettant en avant une description d'un protocole pour les réseaux MANET, ses avantages et limitations devraient être mentionnés de sorte que les contextes appropriés pour son utilisation puissent être identifiés.

Les protocoles de routage doivent être évalués afin de mesurer les performances de la stratégie utilisée et de tester sa fiabilité. L'utilisation d'un réseau Ad hoc réel dans une évaluation est difficile et coûteuse, en outre de telles évaluations ne donnent pas généralement des résultats significatifs. Le réseau réel n'offre pas la souplesse de varier les différents paramètres de l'environnement et pose en

plus le problème d'extraction de résultats; c'est pour cela que la majorité des travaux d'évaluation de performances utilisent le principe de simulation vu les avantages qu'il offre.

Les paramètres mesurés dans une évaluation dépendent de la stratégie de routage appliquée (par exemple dans le cas où on veut comparer deux versions d'un même protocole), mais généralement tout simulateur doit être en mesure d'évaluer :

(a) Le contrôle utilisé dans le mécanisme de mise à jour de routage ;

(b) Les délais moyens du transfert des paquets ;

(c) Le nombre moyen de nœuds traversés par les paquets de données.

II.7. Classification des protocoles de routage Ad hoc

II.7.1. Différents critères de classification

Dans la littérature, et selon certains critères, plusieurs classifications [8] des protocoles de routage unicast dans les réseaux Ad hoc ont été données (figureII.2), on peut citer :

- Classification selon la manière de créer et de maintenir des routes lors de l'acheminement des données, en trois types : protocoles proactifs, protocoles réactifs et protocoles hybrides ;
- Classification basée sur la vision que les protocoles de routage ont sur le réseau et le rôle qu'ils assignent aux différents noeuds mobiles afin de construire la topologie de cheminement. En se basant sur cette philosophie, les protocoles peuvent être classés en protocoles hiérarchiques et protocoles plats ;
- Classification des protocoles de routage selon certaines caractéristiques de localisation ; deux catégories peuvent être distinguées : les protocoles PLI (Physic Location Information) et les protocoles ALI (Approximante Location Information).

II.7.2. Classification générale

Parmi les différentes classifications citées ci-dessus, la plus générale est celle qui classe les protocoles de routage selon la manière de création et de maintenance des routes lors l'acheminement des données, dont les catégories distinguées sont :

II.7.2.1. Protocoles proactifs (Table driven routing protocols)

Les protocoles proactifs sont basés sur la même philosophie que les protocoles de routage utilisés dans les réseaux filaires. C'est-à-dire qu'ils sont fondés sur la méthode état de lien et vecteur de distance.

Avec ces protocoles, chaque nœud maintient une ou plusieurs tables qui permettent d'atteindre tous les autres nœuds du réseau. Chaque nœud met à jour ces informations régulièrement. Lorsque la topologie du réseau évolue, les nœuds diffusent des messages de mise à jour à travers tout le réseau. L'avantage que présente ce type de protocoles est la disponibilité immédiate des routes quand les applications en ont besoin. Néanmoins, la procédure engendre un coût d'échanges supplémentaire qui consomme plus de bande passante inutilement, puisque seules certaines routes seront utilisées.

Les protocoles de cette famille se différencient par la manière dont cette information de mise à jour est transmise à travers le réseau ainsi que le nombre de tables de routages utilisées.

Actuellement ils existent plusieurs protocoles proactifs comme DSDV, OLSR, WRP, GSR et FSR qui seront détaillés dans le paragraphe I.8.1.

II.7.2.2. Protocoles réactifs (On demande routing protocols)

Les protocoles de routage réactifs représentent les protocoles, les plus récents, proposés dans le but d'assurer le service du routage dans les réseaux sans fil.

Les protocoles de routage appartenants à cette catégorie, créent et maintiennent les routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte de route est lancée, et cela dans le but d'obtenir une information spécifiée, inconnue au préalable. Avec cette manière de construction des routes, il y aura moins de trafic de contrôle, ce qui permet d'économiser de la bande passante et de l'énergie. L'aspect négatif réside dans l'introduction d'un temps de latence supplémentaire lors la recherche des chemins.

Dans cette famille plusieurs protocoles existent déjà dont DSR, AODV, TORA, LAR et RDMAR seront décrit dans le paragraphe II.8.2.

II.7.2.3. Protocoles hybrides

Cette troisième approche consiste à utiliser un mélange des techniques proactives et réactives. En général ces protocoles vont fonctionner dans l'un ou l'autre mode suivant des conditions prédéfinis. On peut garder la connaissance locale de la topologie jusqu'à un nombre prédéfini de sauts par un échange périodique de messages de contrôle, c'est à dire par une technique proactive. Les routes vers des nœuds plus lointains seront obtenues par schéma réactif, c'est à dire par l'utilisation de paquets de requête en diffusion.

II.7.2.4. Comparaison des approches

Les protocoles de routage proactifs :

- Sont des grands consommateurs de bande passante et donc d'énergie;
- Connaissent l'information quand instantanément.

À l'inverse, les protocoles de routage réactifs :

- Construisent l'information au moment où on en a besoin;
- Peu consommateurs de bande passante et donc d'énergie.

Intuitivement, on peut penser que la sécurisation potentielle des protocoles proactifs est plus forte étant donné leur caractère précis. En effet, sous une telle hypothèse, il est plus facile d'observer l'état des noeuds (en service, en déplacement).

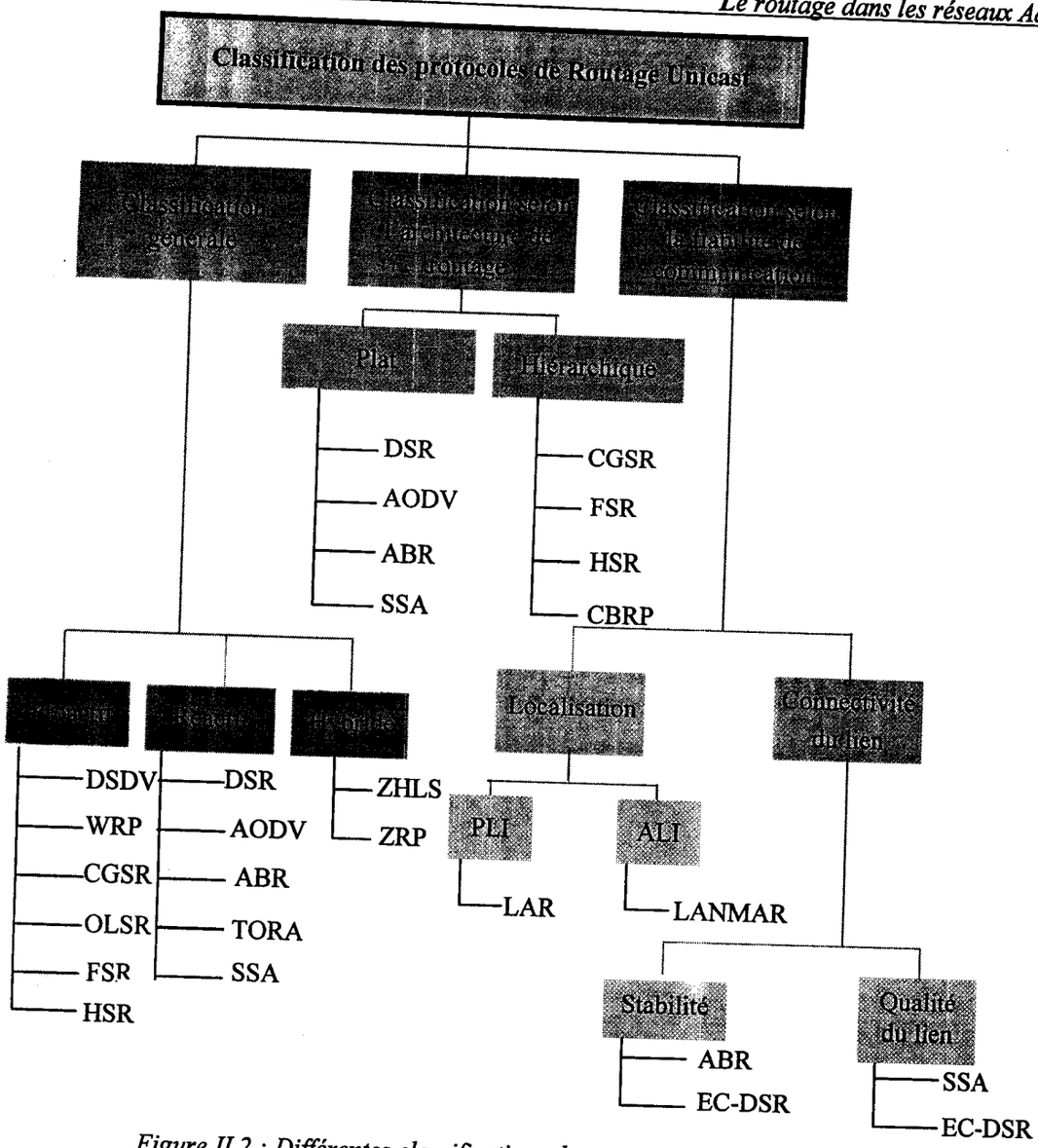


Figure II.2 : Différentes classifications des protocoles de routage Ad hoc

II.8. Description de quelques protocoles de routage

II.8.1. Protocoles proactifs

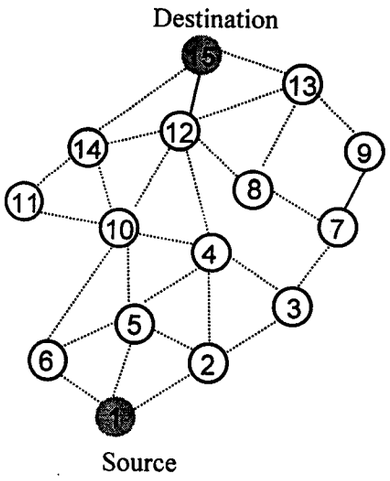
II.8.1.1. Protocole DSDV (Dynamic Destination-Sequenced Distance Vector)

DSDV [8] est un protocole de routage à vecteur de distance, a été conçu spécialement pour les réseaux mobiles. Il est basé sur l'idée classique de l'algorithme distribué de Bellman-Ford. Chaque noeud mobile maintient une table de routage qui contient, pour toutes les destinations possibles, le nombre de nœud (ou de sauts) nécessaire pour les atteindre et le numéro de séquences (SN : sequence number) qui correspond à un nœud destination. Le SN est utilisé pour faire la distinction entre les anciennes et les nouvelles routes, ce qui évite la formation des boucles de routage

Les mises à jour des tables de routage sont périodiques et dès qu'un évènement important arrive. D'où l'utilisation de deux types de mises à jour : une mise à jour complète (quand le nœud transmet la totalité de la table routage aux voisins); et une mise à jour partielle (l'envoi, juste des entrées qui ont subit un changement par rapport à la dernière mise à jour, ce qui réduit le nombre de

paquets transmis). Les données de routage reçues par une unité mobile, sont comparées avec les données déjà disponibles. La route étiquetée avec la plus grande valeur du numéro de séquence (i.e. la route la plus récente), est la route utilisée. Si deux routes ont le même numéro de séquence, alors la plus courte route (shortest path) sera utilisée

Le DSDV élimine les deux problèmes de boucle de routage "routing loop", et celui du "counting to infinity". Cependant, ce protocole est lent, du fait qu'une unité mobile doit attendre jusqu'à ce qu'elle reçoive la prochaine mise à jour initiée par la destination, afin de mettre à jour l'entrée associée à cette destination, dans la table de routage.



Destination	Prochain saut	Distance	SN
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

a- Topologie du réseau *b- Tableau de routage du noeud* **1**

Figure II.3 : Exemple d'une table de routage pour le protocole DSDV

II.8.1.2. Protocole WRP (Wireless Routing Protocol)

Dans ce protocole [12], chaque nœud maintient quatre tables : une table des distances, une table de routage, une table de coût, et une liste MRL (Message Retransmission List). La table des distances garde une trace des distances vers les différentes destinations. La table de routage maintient pour chaque destination, la distance à cette destination, le premier nœud après la source sur le chemin à la destination et le prédécesseur de la destination. La table de coût maintient le coût des liens vers les voisins. Finalement, le MRL détermine quelles mises à jour doivent être retransmises, quand ces retransmissions doivent avoir lieu, et quels voisins devraient acquitter les retransmissions

Le WRP est caractérisé par sa vérification de la consistance des voisins, à chaque fois où un changement d'un lien voisin est détecté. La manière avec laquelle le WRP applique la vérification de la consistance, aide à éliminer les situations des boucles de routage et à minimiser le temps de convergence du protocole.

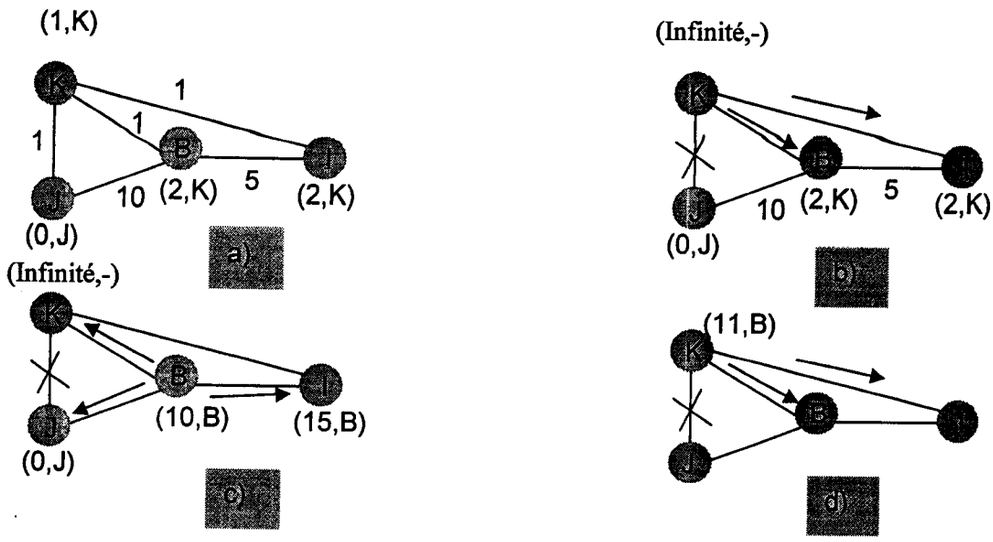


Figure II.4 : Les opérations du WRP

II.8.1.3. Protocole OLSR (Optimazed Link State Routing)

Afin de maintenir à jour les tables de routage, chaque noeud implémentant OLSR [12] diffuse régulièrement des informations sur son propre voisinage. Ces informations sont suffisantes pour permettre à chaque noeud de reconstruire une image du réseau et de trouver une route vers n'importe quelle destination. Mais, cette diffusion ne se fait pas par une simple inondation, où chaque noeud retransmet simplement chaque nouveau paquet qu'il reçoit, OLSR optimise la diffusion grâce au système des relais multi-points MPR (Multi-Points Relays). Chaque noeud choisit dans ses voisins directs un sous-ensemble minimal de noeuds qui lui permettent d'atteindre ses lointains voisins à deux sauts. La diffusion des informations sur les liens utilisés pour le routage se fait ensuite uniquement par les relais multi-points ; la couverture totale du réseau est assurée tout en limitant sensiblement le nombre de ré-émissions. Afin de choisir ses relais multipoints, un noeud a besoin de connaître complètement la topologie de son voisinage à deux sauts ; cela est réalisé grâce à l'envoi périodique de paquets « hello » contenant la liste des voisins connus à un saut.

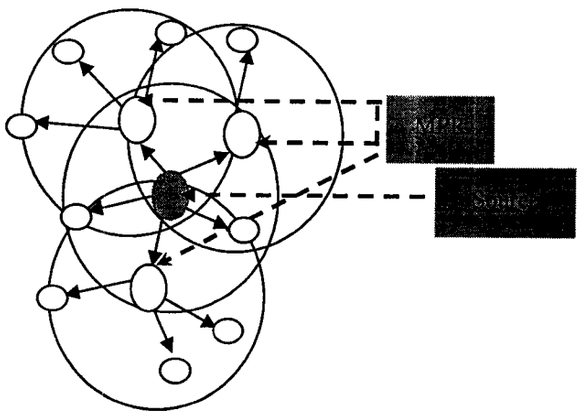


Figure II.5 : Relais multipoints dans le protocole OLSR

II.8.1.4. Protocole GSR (Global State Routing)

Ce protocole est similaire à DSDV, il utilise les idées du routage basé sur l'état des liens, et les améliore en évitant le mécanisme de l'inondation des messages de routage. Le GSR [12] utilise une vue globale de la topologie du réseau. Chaque nœud maintient : une liste de voisins , une table de topologie, une table des nœuds suivants et une table de distance. La table de la topologie, contient pour chaque destination, l'information de l'état des liens telle qu'elle a été envoyée par la destination. Pour chaque nœud de destination, la table des nœuds suivants contient le nœud, vers lequel les paquets de la destination seront envoyés. La table de distance, contient la plus courte distance pour chaque nœud destination.

II.8.1.5. Protocole FSR (Fisheye State Routing)

Ce protocole [12] constitue une amélioration de GSR, il est basé sur l'utilisation de la technique d'œil de poisson, proposée dans le but de réduire le volume d'information nécessaire pour représenter les données graphiques. GSR utilise une diffusion des informations avec une fréquence qui dépend du nombre de sauts pour atteindre les autres nœuds. Par conséquent, un nœud a des informations précises sur ses voisins et la précision de l'information diminue lorsque la distance des nœuds à atteindre augmente. Les niveaux de précision du nœud central dépendent du nombre de sauts pour atteindre un autre nœud. Même lorsqu'il ne dispose pas d'informations précises sur le nœud à joindre, le routage s'effectue correctement car l'information de routage devient de plus en plus en plus précise au fur et à mesure que les paquets se rapprochent de leur destination.

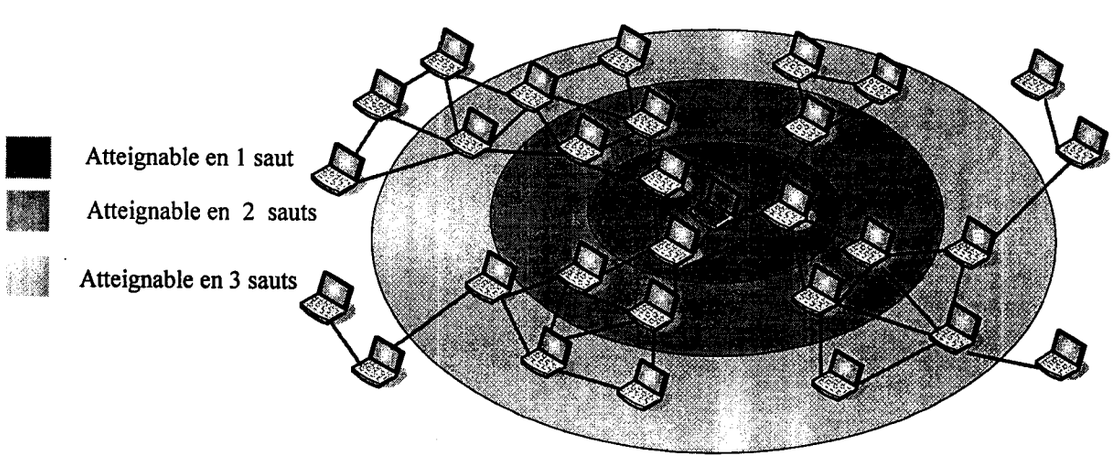


Figure II.6 : Représentation de l'œil de poisson dans un réseau Ad hoc

I.8.2. Protocoles réactifs

II.8.2.1. Protocole DSR (Dynamic Source Routing)

Le protocole DSR [12] utilise la technique du routage source et repose sur des mécanismes de découverte et de maintenance de route. Si un destinataire est dans la cache du nœud source, la route connue est utilisée, sinon une découverte de route est déclenchée. Afin d'envoyer un paquet de donnée au destinataire, l'émetteur construit une route source et l'inclut dans l'en tête du paquet. La construction se fait en spécifiant l'adresse de chaque nœud à travers lequel le paquet va passer pour

atteindre la destination. Par la suite, l'émetteur transmet le paquet, à l'aide de son interface, au premier nœud spécifié dans la route source. Un nœud qui reçoit le paquet, et qui est différent de la destination, supprime son adresse de l'en tête du paquet reçu et le transmet au nœud suivant identifié dans la route source. Ce processus se répète jusqu'à ce que le paquet atteigne sa destination finale.

Afin d'assurer la validité des chemins utilisés, DSR exécute une procédure de maintenance des routes. Quand un nœud détecte un problème fatal de transmission, un message erreur de route (route error) est envoyé à l'émetteur original du paquet. Le message d'erreur contient l'adresse du nœud qui a détecté l'erreur et celle du nœud qui le suit dans le chemin. Lors de la réception du paquet erreur de route par l'hôte source, le nœud concerné par l'erreur est supprimé du chemin sauvegardé, et tous les chemins qui contiennent ce nœud sont tronqués à ce point là. Par la suite, une nouvelle opération de découverte de routes vers la destination, est initiée par l'émetteur.

Parmi les avantages du protocole DSR, le fait que les nœuds intermédiaires n'aient pas besoin de maintenir les informations de mise à jour pour envoyer les paquets de données, puisque ces derniers contiennent toutes les décisions de routage. En outre, dans ce protocole, il y a une absence totale de boucle de routage, car le chemin source destination fait partie des paquets de données envoyés.

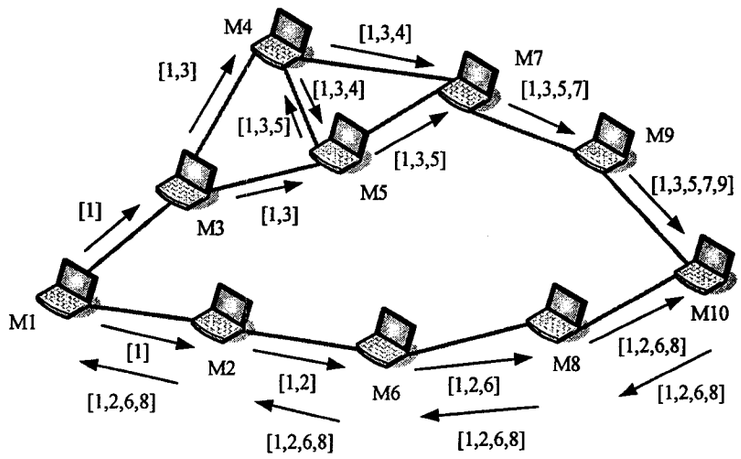


Figure II.7 : Principe de découverte de route par DSR

II.8.2.2. Protocole AODV (Ad hoc On demand Distance Vector)

AODV [11] est un protocole basé sur l'algorithme de vecteur de distance. Il propose une amélioration du protocole DSDV qui consiste à limiter le nombre d'informations de routage sur le réseau. Lorsqu'un nœud cherche une route vers une destination, il diffuse une demande de route à travers le réseau. Les nœuds qui reçoivent ces paquets, les diffusent à leur tour jusqu'à atteindre un nœud qui possède une information de routage récente vers la destination recherche ou la destination elle-même. Les nœuds qui relaient des informations de routage mettent également à jour leurs informations de routage.

Pour que le routage fonctionne efficacement, chaque nœud dans le réseau doit se conformer à un ensemble de règles constituant l'algorithme AODV. Tous les nœuds acceptent de faire router les paquets de données et les informations de routage même s'ils ne sont pas directement impliqués dans

le paquet transmis. Un nœud source souhaitant communiquer avec un nœud destinataire doit d'abord consulter sa table de routage. S'il ne trouve pas localement toutes les informations sur la route à suivre ; il diffusera un message de demande de route (route request message ou rreq) aux nœuds voisins.

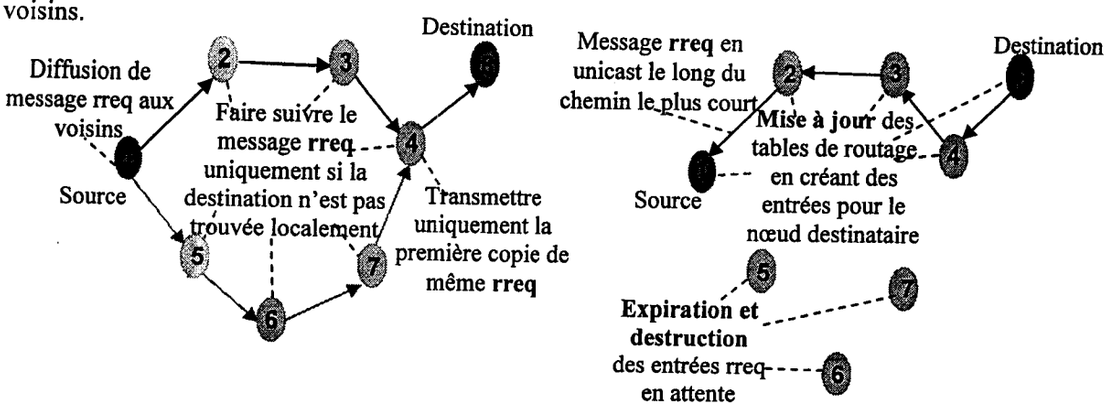


Figure II.8 : Fonctionnement du protocole AODV

II.8.2.3. Protocole TORA (Temporary Ordering Routng Algorithm)

TORA [12] cherche à limiter la quantité de signalisation dans le réseau, par exemple, lorsqu'un changement s'opère dans le réseau, les messages de signalisation de l'évènement ne sont propager que vers des nœuds proches. Une source a toujours plusieurs chemins vers une destination. Pour cela, les nœuds maintiennent des informations de routage vers leurs voisins. Il existe trois catégories de message de routage : création de route, mise à jour de route et effacement de route. La création de route est effectuée par diffusion d'un message QRY (query) qui contient l'identifiant du destinataire. Lorsque ce message atteint un nœud qui connaît la destination un message UPD (update) de mise à jour de route contenant les informations locales sur la destination est envoyé à la source. La métrique reçue est stockée et envoyée aux voisins. Ceci permet de construire un graphe dirigé et acyclique de la source à la destination. Lorsque la topologie change, des mises à jour sont envoyées dans le réseau. Lorsque des routes ne sont plus valides, elles sont effacées dans tout le réseau par une diffusion des messages d'effacement de route.

TORA est un protocole adapté pour de grands réseaux ayant des nœuds fortement mobiles et disposant de ressource limitée en bande passante, il donne plusieurs routes sans boucle mais n'apporte pas l'assurance de trouver une route optimale en termes du nombre de sauts minimum.

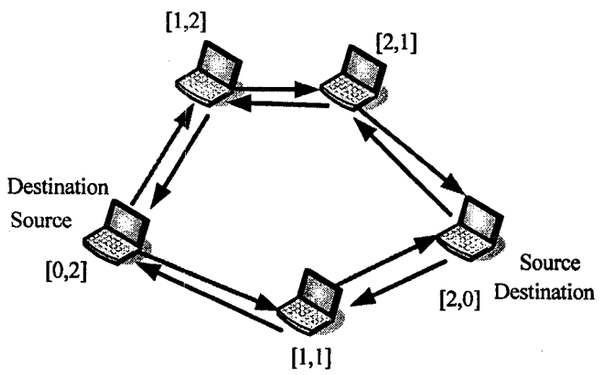


Figure II.9 : Taille des nœuds avec TORA

II.8.2.4. Protocole LAR (Location-Aided Routing)

Le protocole LAR [8] est similaire au protocole DSR, avec une principale différence résidant dans le fait que LAR exploite les informations des localisations, fournies par un GPS et les utilise pour limiter l'inondation des paquets de requête de route, dont deux approches sont utilisées.

La première consiste à ce que le nœud source définit une région de localisation circulaire de la destination, dont la position et la taille sont estimées en fonction de : la position de la destination, l'instant qui correspond à cette position et la vitesse moyenne de déplacement de la destination.

Dans la deuxième approche, le nœud source calcule la distance qui le sépare de la destination, et l'inclut dans un paquet de requête de route envoyé aux nœuds voisins. Quand un nœud reçoit le paquet de requête, il calcule, de son tour, la distance restante pour atteindre la destination, et la compare avec la distance contenue dans le paquet. Ce dernier sera envoyé si la distance calculée est inférieure ou égale à la distance reçue et le nœud mettra à jour le champ de distance.

Si aucune réponse de route n'est reçue, après une certaine période (timeout period), le nœud source rediffuse une nouvelle requête de route en utilisant une diffusion sans limitation.

II.8.2.5. Protocole RDMAR (Relative Distance Micro-discovery Ad hoc Routing)

Le protocole RDMAR été conçu principalement pour minimiser la charge induite par les changements rapides des réseaux Ad hoc. Le protocole utilise un nouveau mécanisme de découverte de routes, appelé la Micro découverte de Distance Relative ou RDM (Relative Distance Micro-discovery). L'idée de base du RDM est la diffusion des requêtes qui peut se faire à base d'une distance relative (RD) entre les paires des unités mobiles. Un algorithme itératif est utilisé pour estimer la RD qui sépare les deux noeuds, et cela en utilisant les informations concernant la mobilité des noeuds, le temps écoulé depuis la dernière communication et l'ancienne valeur de la distance RD. Sur la base de la nouvelle distance calculée, la diffusion de requête est limitée à une certaine région du réseau dans laquelle la destination peut être trouvée. Cette limitation de diffusion, peut minimiser énormément le contrôle du routage, ce qui améliore les performances de la communication.

Dans ce protocole, la décision du choix de chemin est prise au niveau du noeud destination, avec une validation du meilleur chemin, les autres chemins restent passifs. Si un nœud détecte une défaillance d'un lien, il exécute une phase d'avertissement de défaillance afin d'avertir la source de l'invalidité du lien concerné.

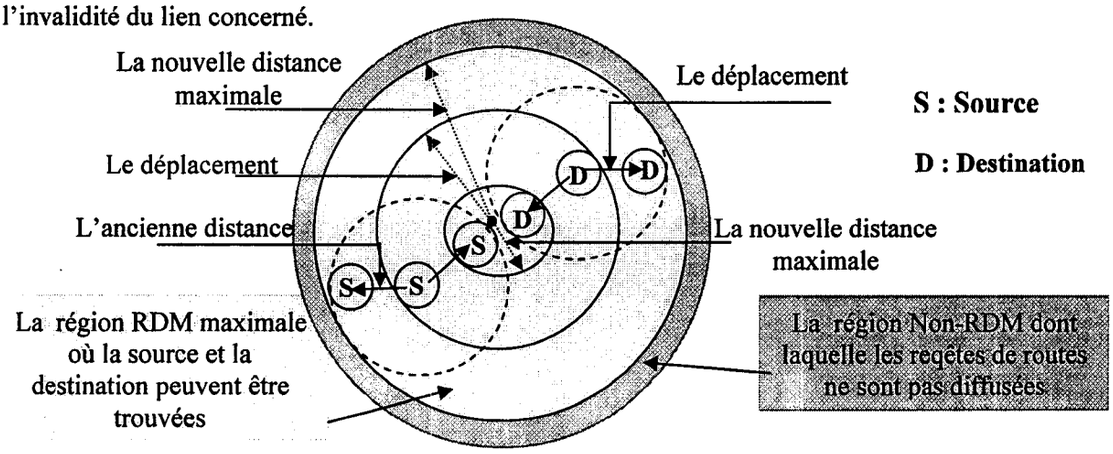


Figure II.10 : Le mécanisme des Distances Relatives du protocole RDMAR

II.8.3. Protocoles hybrides

II.8.3.1. Protocole ZRP (Zone Routing Protocol)

ZRP [11-12] introduit le mécanisme de zone de routage, qui consiste à définir, pour chaque nœud, une zone comportant une taille de rayon correspondant à certaine valeur, de nombre de saut, fixée par l'administrateur du réseau. Les nœuds situés sur la frontière de la zone sont appelés nœuds périphériques et serons utilisés pour trouver les routes vers des nœuds externes de la zone définie. ZRP a deux types de fonctionnement : IARP (IntrAzone Routing Protocol) et IERP (IntErzone Routing Protocol).

IARP donne, d'une manière proactive basée sur le routage par vecteur de distance, toutes les routes jusqu à la frontière de la zone de routage. Pour atteindre les destinations en dehors de cette zone, IERP donne de façon réactive les routes nécessaires.

Le processus de recherche de route fonctionne comme suit. Si une route est connue cela signifie que la destination est à l'intérieure de la zone de routage, si aucune route n'est connue cela signifie que le nœud est à l'extérieure de cette zone. Dans ce cas le nœud envoie une requête par IERP à tous ses nœuds de périphérie. Si un nœud périphérique connaît une route il renvoie une réponse sinon le protocole se poursuit récursivement jusqu'à obtention d'une route.

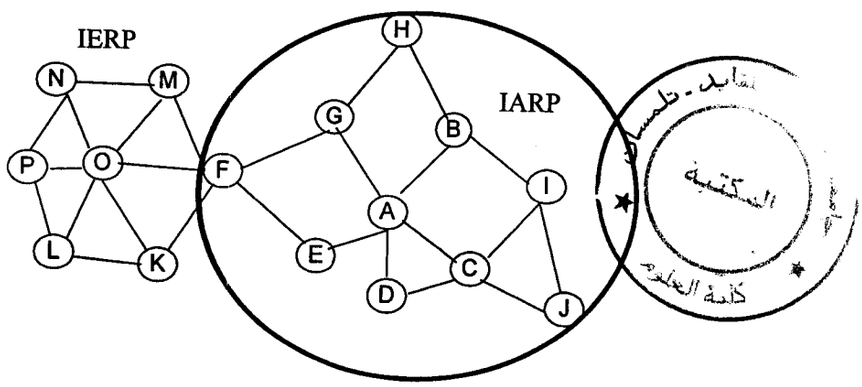


Figure II.11 : Fonctionnement du protocole ZRP

II.8.3.2. Protocole CBRP (Cluster Based Routing Protocol)

Dans CBRP [11], le réseau est décomposé en groupes, constitués de nœud membres et d'un représentant. Un nœud sans statut (ni membre, ni représentant) active un timer et diffuse un message « HELLO », si ce message est reçu par un représentant d'un groupe, le nœud reçoit une réponse immédiate lui donnant l'accord de devenir membre de ce groupe, à condition que l'attente de la réponse n'ait pas dépassée le timeout, si ce dernier est dépassé et le nœud possède au moins un lien bidirectionnel vers un nœud voisin, le nœud peut, dans ce cas, se proclamer représentant d'un groupe. Sinon il reste toujours sans statut et répète la procédure.

Les nœuds maintiennent une table des voisins dont chaque entrée est associée à un voisin, en indiquant son statut et l'état du lien (uni ou bidirectionnel). Le représentant d'un groupe regroupe les informations concernant les membres de son groupe et possède une table dont chaque entrée est

associée à un groupe adjacent et contient l'identificateur du groupe, l'identificateur du nœud de son groupe permettant la liaison avec ce groupe et l'identificateur du représentant de ce groupe.

Un représentant, d'un groupe, qui reçoit une requête de demande de route, vérifie, dans sa table des membres, s'il s'agit d'une destination de son groupe, si le membre est trouvé il lui envoie directement la requête, sinon la requête sera transmise vers les représentants des groupes voisins. Quand la requête parvient au destinataire, celui-ci répond par l'envoi du chemin qui a été sauvegardé dans le paquet de la requête. Si le nœud source ne reçoit pas de réponse au bout d'une certaine période, il envoie de nouveau la requête.

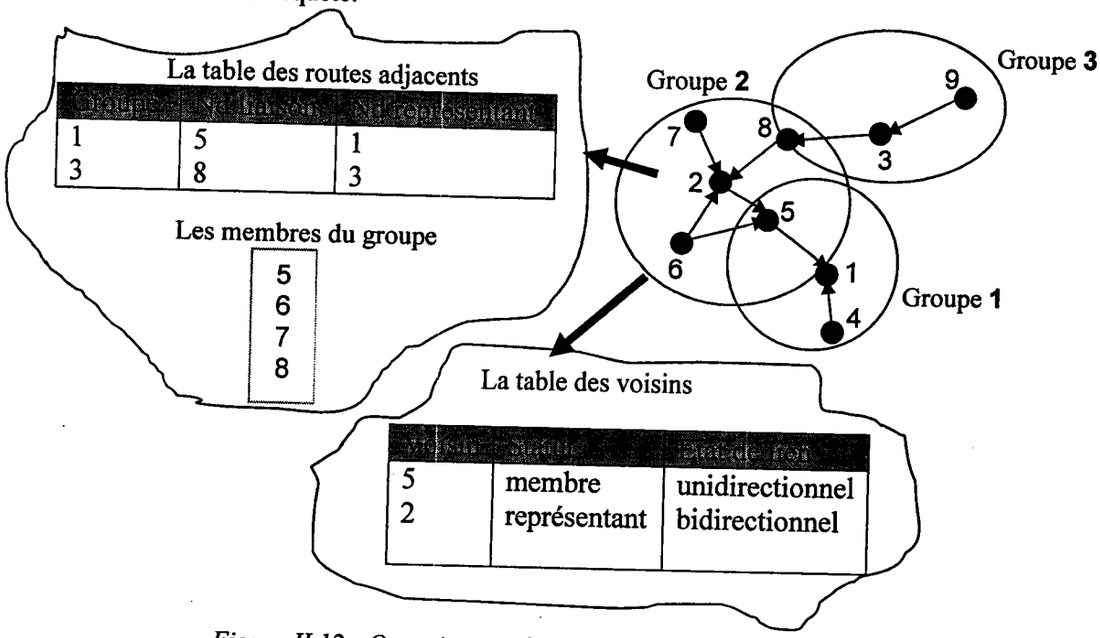


Figure II.12 : Organisation du réseau dans le protocole CBRP

II.9. Extensions des protocoles de routage

Les algorithmes de routage ont été conçus, essentiellement, pour router les données sans tenir compte des contraintes spécifiques de qualité de service, de sécurité et d'efficacité énergétique. Pour répandre à ces exigences, plusieurs extensions de ces protocoles ont été proposées.

II.9.1. Protocoles de routage avec qualité de service

Le but des protocoles de routage avec la qualité de service [13] est de trouver une route ayant suffisamment de ressources pour satisfaire les besoins de QoS d'une communication, tout en optimisant l'utilisation des ressources disponibles. Dans ce sens, différents protocoles ont été développés, on peut citer :

- ***CEDAR (Core-Extraction Distributed Ad hoc Routing Algorithm):***

CEDAR [13] est un protocole de routage réactif. Au lieu de calculer une route avec un minimum de saut, l'objectif principal de CEDAR est de trouver un chemin stable pour garantir plus de bande passante. Dans ce protocole de routage, les noeuds du coeur du réseau auront plus de trafics à gérer, en plus des messages de contrôle (pour la découverte et la maintenance des routes). En outre, en cas de forte mobilité, la convergence de l'algorithme est difficile à atteindre. Il est basé sur trois composantes essentielles :

❖ L'extraction d'un coeur du réseau, par le choix d'un ensemble de noeud pour calculer les routes et maintenir l'état des liens du réseau;

❖ La propagation d'état de lien pour informer les noeuds distants sur les liens stables avec une grande bande passante;

❖ Le calcul de route qui est basé sur la découverte et l'établissement d'un plus court chemin vers la destination satisfaisant la bande passante demandée. Des routes de 'secours' sont utilisées lors de la reconstruction de la route principale, quand cette dernière est perdue.

• ***Extension du protocole DSR***

Plusieurs extensions du protocole DSR pour la QoS sont proposées :

❖ Extension du protocole DSR par la différenciation des stations, qui exploite la possibilité offerte d'avoir plusieurs routes dans son cache, et consiste à ajouter les types des noeuds et à modifier la procédure de sélection de route.

❖ Une implémentation du DSR avec de QoS [13] dans un environnement utilisant des communications TDMA synchrones.

❖ Multipath QoS à base du DSR [13] conçu pour fonctionner dans un environnement CDMA, permet à un nœud de chercher des chemins multiples qui satisferont certaines exigences de bande passante.

• ***Extension du protocole AODV***

Une extension proposée dans [14] consiste à étendre les paquets « route request » et « route response » durant la phase de découverte de la route. De plus, les informations suivantes sont ajoutées dans la table de routage : bande passante minimale, délai maximum, et la liste des sources qui ont demandé des garanties de délai ou de bande passante. Si un nœud détecte que la QoS demandée n'est pas satisfaite alors il envoie un message à la source ayant initiée cette demande de QoS, pour l'informer.

• ***Autres extensions des protocoles de routage pour la QoS***

❖ Des extensions du protocole TORA : tels que : le protocole QoS-TORA, et le protocole INORA qui utilise le protocole INSIGNIA (in-band signalling) pour la signalisation et TORA pour le routage ;

❖ Des extensions du protocole DSDV : tels que MAC (RTMAC), et le protocole MACA/PR (Multiple Access Collision Avoidance/ Piggy-back Reservation) .

II.9.2. Extensions pour la sécurité

Dans les réseaux Ad hoc, la sécurité concerne deux aspects : la sécurité du routage et la sécurité des données.

Un protocole détaillé dans, appelé SRP (Secure Routing Protocol) est proposé comme solution contre les comportements malveillants dont l'objectif est la découverte des informations de topologie ou l'injection de fausses informations de routage. SRP a été conçu pour fournir des informations de routage correctes (effectif, mises à jour et assure l'authentification entre noeuds qui désirent communiquer d'une façon sécurisée). SRP permet de découvrir une ou plusieurs routes dont on peut

vérifier l'authenticité. Des requêtes de route (route requests) se propagent à la recherche de destinations de confiance. Les réponses de route (route replies) sont retournées, strictement, sur la route inverse, accumulée dans les paquets de requêtes de route.

Le centre de recherches de Nokia, de son coté, a développé des spécifications pour l'amélioration du protocole AODV, le protocole résultant est appelé (SAODV : Secure AODV) [15]. Le protocole SAODV peut être employé pour protéger le mécanisme de découverte d'itinéraire en fournissant des dispositifs de sécurité comme l'intégrité, l'authentification et la non répudiation des messages de cheminement.

En outre, pour la détection des intrusions, les auteurs développent une architecture de détection d'intrusion et évaluent un mécanisme de clés pour la détection d'anomalies dans les réseaux mobiles Ad hoc, utilisant des simulations. Des résultats expérimentaux, données par les auteurs utilisant les protocoles de routage : DSR, AODV et DSDV, démontrent que cette approche de détection d'anomalies peut fonctionner dans différents types de réseaux Ad hoc, mais il y a quelques limitations sur la capacité de détection par rapport au degré de mobilité des noeuds.

II.9.3. Extensions pour la gestion de l'énergie

Les protocoles de routage affectent clairement la consommation d'énergie dans les réseaux Ad hoc où chaque mobile émet plusieurs messages puisqu'il doit, à la fois, transmettre ses propres données mais, également, les données des autres mobiles pour lesquels il fait office de routeur, c'est la raison pour laquelle l'économie d'énergie devient une question critique traitée dans les travaux de recherches effectuées dans le cadre des réseaux Ad hoc.

De nombreux protocoles de routage basés sur l'énergie sont proposés dans la littérature, on peut donner comme exemple, les protocoles qui reposent sur les protocoles existant déjà : le protocole DSR (Energy Conserving, Energy Aware, Energy Depended, Mimum Drain Rate,...) [8], le protocole AODV (Localized Energy Aware Routing, Power Aware Routing), les nouveaux protocoles comme SPAN (power Saving Protocol for Ad hoc Network) et GAF (Geographic Adaptive Fidelity), ...Ces protocoles seront détaillés dans le chapitre trois.

II.10. Conclusion

Dans ce chapitre nous avons présenté le routage dans les réseaux Ad hoc. Nous avons vu que l'étude et la mise en oeuvre des protocoles de routage pour assurer la connexion des réseaux Ad hoc au sens classique, est un problème très compliqué en raison des limitations imposées par l'environnement. Donc les stratégies de routage doivent en tenir compte, et afin de tester la fiabilité et l'efficacité de la solution proposée, une évaluation de performances doit être faite. Ainsi, nous avons donné un état de l'art de la classification des différentes approches utilisées pour résoudre ce problème, la classification la plus générale a pris en considération la manière avec laquelle les routes sont crées et maintenues et distingue trois types de familles : les protocoles proactifs, les protocoles réactifs et les protocoles hybrides. Ceci a été suivi par une description de quelques protocoles de chaque famille.

Nous avons vu aussi que ces protocoles, conçus essentiellement pour router les données, peuvent avoir des extensions pour tenir compte des contraintes spécifiques ou à des demandes des utilisateurs. En effet, nous avons prendre le protocole OLSR concernent la qualité de service, le principe de fonctionnement de protocole. Cette dernière sera traitée en détail dans le troisième chapitre.

Chapitre III

Le protocole de routage à état de optimisé OLSR

III.1.Introduction

Plusieurs efforts de recherche ont été entrepris ces dernières années visant à développer des protocoles pour des réseaux devant fonctionner sans un contrôle central et faisant appel aux nœuds pour se connecter directement les uns aux autres pour relayer les messages par des sauts multiples. Ce mode de fonctionnement caractérise les réseaux ad-hoc, pour lesquels l'IETF (Internet Engineering Task Force), a normalisé quelques protocoles de routage dont Optimized Link State Routing Protocol (OLSR).

L'objectif de cet article est d'identifier et de formaliser les hypothèses de confiance utilisées implicitement dans le protocole OLSR. Un des buts de cette analyse est de proposer des extensions au protocole OLSR de façon à le rendre plus flexible aux variations de l'environnement et de le rendre plus résistant aux attaques, tout en évitant de poser des restrictions excessives aux capacités d'auto-organisation et à la dynamicité du réseau.

Pour ce faire, nous partons de l'idée de classification de la confiance, qui consiste en une délimitation des circonstances où une relation de confiance est établie, et procédons à l'analyse des classes de confiance présentes dans ce protocole. Nous présentons en premier lieu le langage utilisé pour exprimer formellement les clauses de confiance, ainsi que la définition de la confiance sous-jacente à ce langage. Ensuite, nous exposons les caractéristiques générales et les problèmes de sécurité du protocole OLSR. Finalement, nous présentons les clauses de confiance implicites à OLSR et analysons les attaques contre ce protocole en fonction de ces clauses implicites.

Dans cet article, nous nous intéressons en particulier à OLSR (Optimized Link State Routing). C'est un protocole proactif, développé essentiellement par le projet HIPERCOM, de l'INRIA, dirigée par Philippe Jacquet. dont une implémentation a été réalisée, permettant de faire des tests en grandeur réelle d'efficacité et de robustesse,

Dans la première section nous décrivons brièvement le protocole de routage OLSR et la technique des relais multipoints.

Puis dans la section suivante, nous soulignons des bases de données ainsi des informations topologiques.

III.2.Terminologie d'OLSR

OLSR est un protocole à état du lien proactif, et non uniforme puisqu'il s'appuie sur une distinction basée sur le voisinage pour établir une hiérarchisation entre les nœuds.

En ce de suite on à présenter les terminologies de ce protocole :

❖ ***Nœud*** Une machine participant au réseau MANET qui met en application le protocole optimisé de cheminement d'état de lien.

❖ ***Interface d'OLSR*** Un dispositif de réseau participant à un MANET utilisant OLSR comme protocole de routage. Un nœud peut avoir plusieurs interfaces d'OLSR, à chaque interface est assignée une adresse IP unique.

❖ ***Non interface d'OLSR*** Un dispositif de réseau, ne participant pas à un MANET utilisant OLSR. Un nœud peut avoir plusieurs non interfaces d'OLSR (sans fil et/ou filaire).

❖ ***Nœud simple d'interface d'OLSR*** Un nœud qui a une seule interface simple d'OLSR.

❖ ***Nœud multiple d'interface d'OLSR*** Un nœud qui possède plusieurs interfaces OLSR.

❖ ***Adresse principale*** L'adresse principale d'un nœud, qui sera employé dans la diffusion des messages d'OLSR comme "l'adresse IP de générateur" de tous les messages émis par ce nœud. C'est l'adresse d'une des interfaces d'OLSR du nœud. Un nœud simple d'interface d'OLSR doit employer l'adresse de son interface d'OLSR comme adresse principale dans toute la diffusion. Un nœud multiple d'interface d'OLSR doit choisir une de ses adresses d'interface d'OLSR en tant que son "adresse principale. Il est sans importance quelle adresse est choisie, toute fois un nœud devrait toujours employer la même adresse que son adresse principale.

❖ ***Nœud voisin*** Un nœud X est un nœud voisin du nœud Y si le nœud Y peut entendre le nœud X (c.-à-d., un lien existe entre une interface d'OLSR sur le nœud X et une interface d'OLSR sur Y).

❖ ***Voisin 2-hop*** Un nœud entendu par un voisin.

❖ ***Relais multipoint (MPR)*** Un nœud qui est choisi par son voisin à un saut. Le nœud MPR retransmet les messages à diffusion générale qu'il reçoit de X.

❖ ***Sélecteur multipoint de relais (sélecteur de MPR, MME.)*** Un nœud qui a choisi quelques voisins à un saut comme MPR.

❖ ***Lien*** Un lien est une paire d'interfaces d'OLSR (de deux nœuds différents) effectuée pour permettre au deux entités OLSR de s'entendre (c.-à-d., on peut pouvoir recevoir le trafic de l'autre).

❖ ***Lien symétrique*** Un lien bidirectionnel vérifié entre deux interfaces OLSR de deux nœuds différents.

❖ ***Lien asymétrique*** Un lien entre deux interfaces OLSR assurant une transmission dans une seule direction.

❖ ***Voisinage 1-hop symétrique*** Le voisinage 1-hop symétrique de n'importe quel nœud X est l'ensemble de nœud qui a au moins un lien symétrique à X.

❖ ***Voisinage 2-hop symétrique*** Le voisinage 2-hop symétrique de X est l'ensemble de nœuds, à l'exclusion de/X> qui ont un lien symétrique au voisinage 1-hop symétrique de X.

❖ ***Inondation*** L'inondation est la technique la plus rudimentaire de diffusion. Elle consiste à répéter un message dans tout le réseau : chaque nœud qui reçoit le message pour la première fois répète le message. Ainsi, de proche en proche, le message inonde le réseau [16].

III.3.Applicabilité

OLSR est un protocole de routage proactif pour les réseaux ad hoc mobiles MANET. Comme OLSR est basé sur la notion des MPR, II est utile dans les réseaux étendus et denses. Plus le réseau est grand et dense plus l'optimisation est réalisée. OLSR demeure bien approprié aux réseaux où le trafic est aléatoire et les nœuds sont à faible mobilité.

III.4.Relais Multipoint

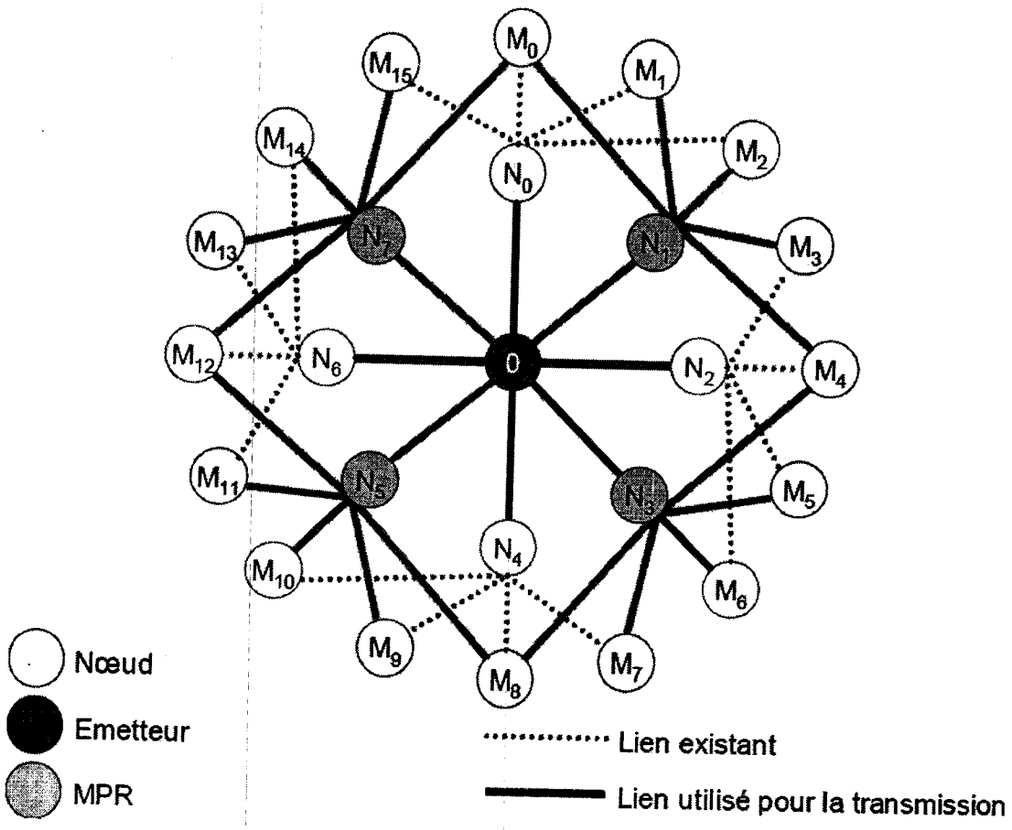


Figure III.1 : Diffusion de messages avec les MP [17]

L'idée des relais multipoint est de réduire au minimum les frais généraux des messages diffusés dans le réseau en réduisant les retransmissions superflus dans la même région. Chaque nœud dans le réseau choisit un ensemble de nœuds dans son voisinage 1-hop symétrique qui peut retransmettre ses messages. Cet ensemble de nœuds voisins choisis s'appelle "le relais multipoint" (MPR).

Chaque nœud choisit son MPR parmi ses voisins 1-hop symétriques. Cet ensemble est choisi tel qu'il couvre tous les nœuds 2-hop symétriques.

L'ensemble des MPR du nœud X, dénoté comme MPR(X), est alors un sous-ensemble arbitraire du voisinage 1-hop symétrique de X qui satisfait la condition suivante : chaque nœud dans le voisinage 2-hop symétrique de X doit avoir un lien symétrique avec MPR(X).

Chaque nœud maintient des informations sur l'ensemble de voisins qui l'ont choisi comme MPR. Cet ensemble s'appelle "MPR Selector Set

L'information exigée pour exécuter le calcul des MPR est acquise par l'échange périodique des messages hello.

On assume qu'un message à diffusion générale, prévu pour être répandu dans le réseau entier, venant de n'importe lequel des sélecteurs de MPR du nœud X est retransmis par le nœud X, si X ne l'a pas reçu encore. .

III.5.Fonctionnement du protocole

Cette section décrit le fonctionnement général du protocole OLSR ;
Dans un souci de simplicité de notre étude, on se mettra dans les hypothèses suivantes :

a. Chaque nœud ne possède qu'une seule interface.

b. Le seul protocole de routage utilisé dans le réseau est OLSR

c. Il n'y a pas d'interface hybride (gateway avec un autre réseau).

III.5.1.Amorçage

Dans un réseau ad hoc chaque machine des sons allumage, effectue les opérations suivantes :

- **La synchronisation** : Un ensemble de bits de let 0 sont échanges au niveau physique.
- **L'association** : Pour participer au réseau ; elle se fait au niveau de la couche MAC.

III.5.2.Encapsulation OLSR

OLSR communique en utilisant un format unifié de paquet pour toutes les données liées au protocole. Ces paquets sont encapsulés dans des datagrammes UDP pour la transmission au-dessus du réseau. Ce dernier à son tour est encapsulé dans un paquet IP.

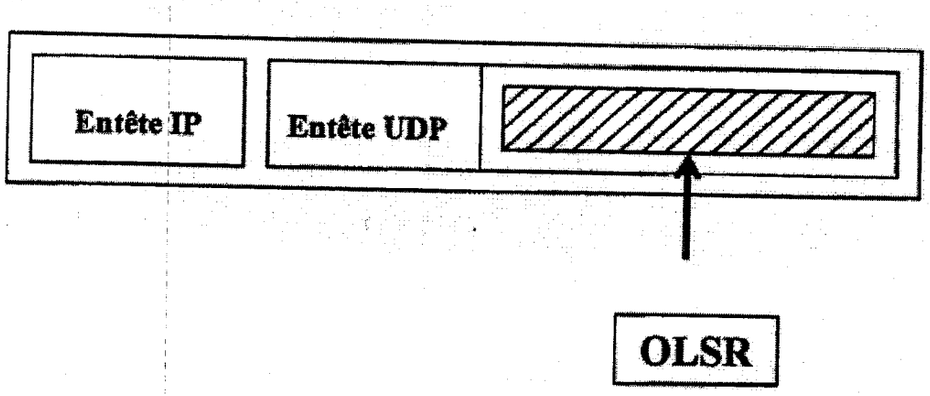


Figure III.2. Encapsulation de protocole OLSR

III.5.3.Format et expédition de paquet

Chaque paquet encapsule un ou plusieurs messages. Les messages partagent un format commun d'en-tête, qui permet à des nœuds de recevoir correctement et retransmettre les messages d'un type inconnu.

Des messages peuvent être inondés sur le réseau entier, ou l'inondation peut être limitée aux nœuds dans un diamètre (en termes de nombre de sauts) du générateur du message. Quand on sert localement l'inondation automatique des différents messages de commande. De ce fait, on évitera la duplication des messages reçus et la charge inutile du réseau (c'est le rôle des MPR).

En outre, un nœud peut examiner l'en-tête d'un message pour obtenir l'information sur la distance (en termes de nombre de sauts) à partir du générateur du message [16].

III.5.4. Protocole et numéro de port

Les paquets dans OLSR communiquent en utilisant l'UDP. Le port 698 a été assigné par IANA pour l'utilisation exclusive par le protocole d'OLSR.

III.5.5.Adresse Principale

Pour un nœud avec une interface, l'adresse principale d'un nœud, comme définie dans la "terminologie d'OLSR", doit être placée à l'adresse de cette interface.

III.5.6.Format du Paquet OLSR

La disposition de base de n'importe quel paquet dans OLSR est comme suit (omettant des en-têtes d'IP et d'UDP).

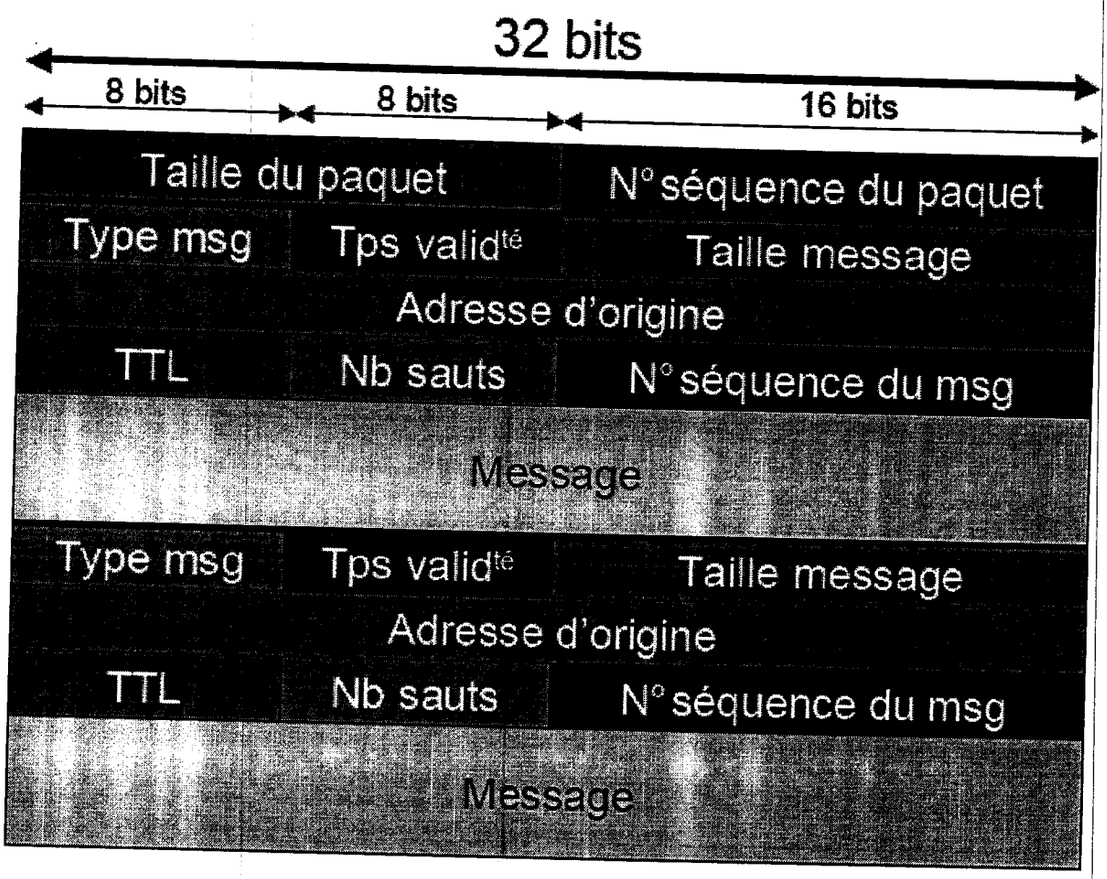


Figure III.3 : Format du paquet OLSR [17]

III.5.6.I.En-tête De Paquet

- **Longueur du Paquet :** La longueur (en bytes) du paquet.
- **Numéro de séquence du Paquet :** C'est un champ de 2 octets qui prend des valeurs de 0 à $(2^{16}-1)$.

Le nombre de séquence de paquet (PSN : Paquet Séquence Number) doit être incrémenté chaque fois qu'un nouveau paquet d'OLSR est transmis. Un nombre de séquence séparé de paquet est maintenu pour chaque interface telle que des paquets transmis au-dessus d'une interface sont séquentiellement énumérés.

Si le paquet ne contient aucun message (c.-à-d., la longueur de paquet est inférieur ou égal à la taille de l'en-tête de paquet), le paquet doit être silencieusement rejeté. Pour les adresses IPv4, ceci implique que des paquets, où la longueur de paquet < 16 doit être silencieusement jetée.

III.5.6.2.En-tête du Message

➢ ***Type de Message***

Ce champ indique quel type de message est encapsulé dans le champ DATA

Il est égal :

- à 1 pour un message de type **hello.**
- à 2 pour un message de type **TC.**

➢ ***Vtime***

Ce champ indique le temps pour le quel un message est considéré comme valide, à moins qu'une mise à jour plus récente de l'information soit reçue. Le temps de validité est représenté par sa mantisse (les quatre bits les plus élevés du champ de Vtime) et par son exposant (les quatre bits les plus bas du champ de Vtime). En d'autres termes :

Temps de validité = $C*(1+a/16) * 2^{A}b$ [en secondes]

Où:

a : est le nombre entier représenté par les quatre bits les plus élevés du champ de Vtime.

b : le nombre entier représenté par les quatre bits les plus bas du champ de Vtime ; La constante proposée pour C est la suivante : C = 1/16 des secondes (égale à 0.0625 seconde).

➢ ***Taille du Message***

Ceci donne la taille du message, comptée en octets et mesurée à partir du commencement du 1^{er} champ « type de message » et jusqu'au le commencement du prochain champ « type de message » est s'il n'y a aucun message suivant on termine jusqu'à l'extrémité du paquet.

➢ ***Adresse de Générateur***

Ce champ contient l'adresse principale du nœud, qui est à l'origine de ce message. Ce champ ne doit pas être confondu avec l'adresse de source de l'en-tête IP, qui est changée chaque fois que ce message est retransmet. La zone Adresse De Générateur ne doit jamais être changée dans les retransmissions.

➢ ***Time to Live (TTL)***

Ce champ contient le nombre maximum de sauts que peut traverser un message avant qu'il soit détruit. Le Time to Live doit être décrémenté par 1 à chaque passage par un nœud. Quand un nœud reçoit un message avec un Time to Live égal à 0 ou à 1, le message ne doit pas être retransmis dans aucune circonstance. Normalement, un nœud ne reçoit pas un message avec TTL égal à zéro. Ainsi, avec ce champ, le générateur d'un message peut limiter le rayon d'inondation.

➢ ***Compte de sauts***

Ce champ contient le nombre de saut traversé par le message. Avant qu'un message ne soit retransmis, le compte de saut doit être incrémenté par 1. Au commencement, ceci est placé à 0 par le générateur du message.

➢ ***Nombre de séquence de Message MSN***

Avant de transmettre les messages, le nœud générateur assignera un numéro d'identification unique à chaque message. Ce nombre est inséré dans le champ de nombre de séquence du message. Le nombre de séquence est augmenté de 1 (un) pour chaque message provenant du nœud. . Ce numéro est utilisé pour éviter la retransmission du message (duplication) ; lors de la réception du message par les MPR set avant de le traiter, ces derniers regardent la DUPLICATE SET c.à.d. regarde si le message est déjà reçu ou non.

III.6.Informations topologiques-Base de données

Par l'échange des messages de commande d'OLSR, chaque nœud accumule des informations sur le réseau. Ces informations sont stockées selon leurs types dans des bases de donné.

III.6.1.Duplicate Set Data Base

Lors de la réception d'un paquet OLSR, un nœud examine chacun des "en-têtes de message". Basé sur la valeur du champ "type de message", le nœud peut déterminer le destinataire du message. Un nœud peut recevoir le même message plusieurs fois. Ainsi, pour éviter le retraitement de quelques messages qui ont été déjà reçus et traités, chaque nœud maintient un ensemble d'information appelé Duplicate Set. Pour un tel message, un noeud enregistre "un tuple double" (Da_ddr, seq_num, Dretransmitted, D_iface_list, D_time) ;

où :

D_addr : est l'adresse de créateur du message ;

D_seq_num : est le nombre d'ordre de message du message,

Dretransmitted : est un booléen indiquant si le message a été déjà retransmis ;

D_iface_list : est une liste des adresses des interfaces sur lesquelles le message a été reçu;

D_time : indique le temps à l'où un tuple expire.

Avant tout traitement, éventuellement retransmission (pour les messages TC), chaque message doit faire l'objet d'une vérification en considération avec la base Duplicate Set

III.6.2.Sensation de Lien : local link information base

La base de donnée local link information base stocke des informations sur les liens existants entre les voisins.

Un noeud enregistre un ensemble de "tuples de lien" :

(L_local_iface_addr, L_neighbor_iface_addr, L_SYM_time, L_ASYM_time, Ljime).

- L_local_iface_addr : est l'adresse d'interface du noeud local);
- L_neighbor_iface_addr : est l'adresse d'interface du noeud voisin ;
- L_SYM_time : est le temps maximum pour lequel le lien est considéré symétrique ;
- L_ASYM_time : est le temps maximum pour lequel le lien est considéré asymétrique
- Ltime : indique le temps d'expiration de ces tuples.

Quand L_SYM_time et L_ASYM_time sont expirés, le lien est considéré perdu.

Cette information est enregistrée par l'échange du message hello.

Dans un nœud, l'ensemble de tuples de lien sont dénotés "ensemble de lien ou Link Set".

III.6.3.Détection du Voisin : Neighbor Hood Information Base

La base de données Neighbor Hood Information Base stocke des informations sur les voisins, les voisins à 2-hop, les MPRs et les sélecteurs de MPR.

➢ ***Ensemble de Voisin***

Un nœud enregistre un ensemble "de tuples voisins" : (N_neighbor_main_addr, N_status, N_willingness).

- N_neighbor_main_addr : est l'adresse principale du voisin ;
- N_status : indique si le nœud est ASYM ou SYM ;
- N_willingness : c'est un nombre entier entre 0 et 7, qui indiquent la bonne volonté du nœud de porter le trafic vers d'autres nœuds (c.à.d. d si le nœud peut transmettre l'information ou pas).

➢ ***Ensemble de Voisin 2-hop***

Un nœud enregistre un ensemble "de tuples 2-hop" : (N_neighbor_main_addr, N_2hop_addr, N_time), décrire des liens symétrique (et, puisque les liens de MPR par définition sont également symétriques, de ce fait aussi les MPR) entre ses voisins et le voisinage 2-hop symétrique.

- N_neighbor_main_addr : est l'adresse principale d'un voisin,
- N_2hop_addr : est l'adresse principale d'un voisin 2-hop avec un lien symétrique à N_neighbor_main_addr,
- N_time indique le temps de validité de cette base de données.

Dans un nœud, l'ensemble de tuples 2-hop sont dénotés "ensemble de voisin a 2-hop".

➢ ***Ensemble de MPR***

Un nœud maintient un ensemble de voisins qui sont choisis comme MPR. Leurs adresses principales sont énumérées dans l'ensemble de MPR.

➢ ***Ensemble de Sélecteur de MPR***

Un nœud enregistre un ensemble de tuples de MPR-sélecteur (MS_main_addr, MS_time), décrivant les voisins qui ont choisi ce nœud comme MPR.

- MS_main_addr est l'adresse principale d'un nœud, qui a choisi ce nœud comme MPR.
- MS_time indique le temps de validité du tuple. Dans un nœud, l'ensemble de tuples de MPR-sélecteur sont dénotés "ensemble sélecteur de MPR" [16].

III.6.4.Topology Information Base

Chaque nœud dans le réseau maintient des informations de topologie sur le réseau. Cette information est acquise par les messages TC et est employée pour des calculs de table de routage.

Ainsi, pour chaque destination dans le réseau, au moins un "tuple de topologie" : (T_dest_addr, T_last_addr, Tseq, T_time) est enregistré.

- T_dest_addr est l'adresse du déstinateur.
- T_last_addr indique l'adresse du MPR de T_dest_addr.
- T_seq c'est le numéro de séquence,
- T_time indique le temps de validité du tuple.
- Dans un nœud, l'ensemble de tuples de topologie sont dénotés "l'ensemble de topologie ou TopologySet".

III.7.Le Message HELLO

Chaque nœud cherche à connaître les interfaces de ses voisins possédant une liaison directe et symétrique avec l'une de ses interfaces. Pour ce faire, les nœuds émettent des paquets de HELLO comportant des informations sur les voisins qu'ils entendent ainsi que la qualité des liens qu'ils entretiennent avec eux. Les liens peuvent avoir quatre états : symétrique Asymétrique, relais multi point (MPR) ou encore perdu. Les messages de type

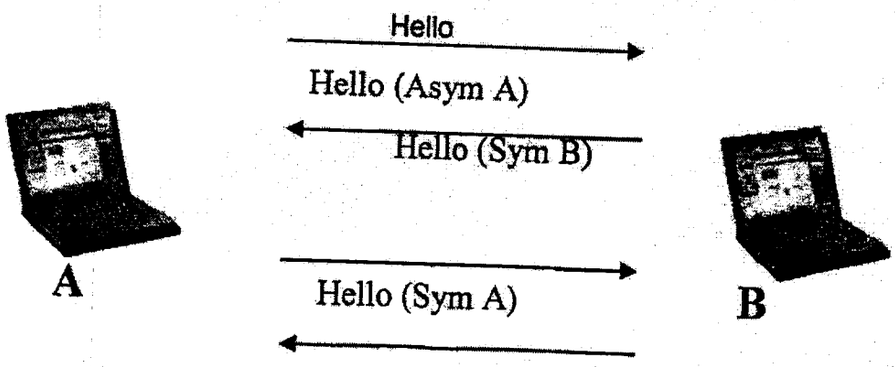


Figure III.4 : Exemple de détection de voisin

Les nœuds de type MPR ou relais multipoints sont désignés par leurs voisins. Dans le cas ou trois machines A, B et C s'entendent deux à deux (A, B) et (B, C) alors A et C choisiront B en relais multipoints afin de pouvoir communiquer. Ils lui indiqueront dans leur prochain message Hello. Bien évidemment, les MPR sont des liens symétriques.

Les liens de type perdus sont détectés lorsque la communication (échange de Hello) n'existe plus entre deux nœuds. Le nœud restant déclare alors dans son prochain message Hello qu'un de ces voisins vient de disparaître.

III.7.1.Format du message HELLO

Le format proposé pour le message Hello est comme suit :

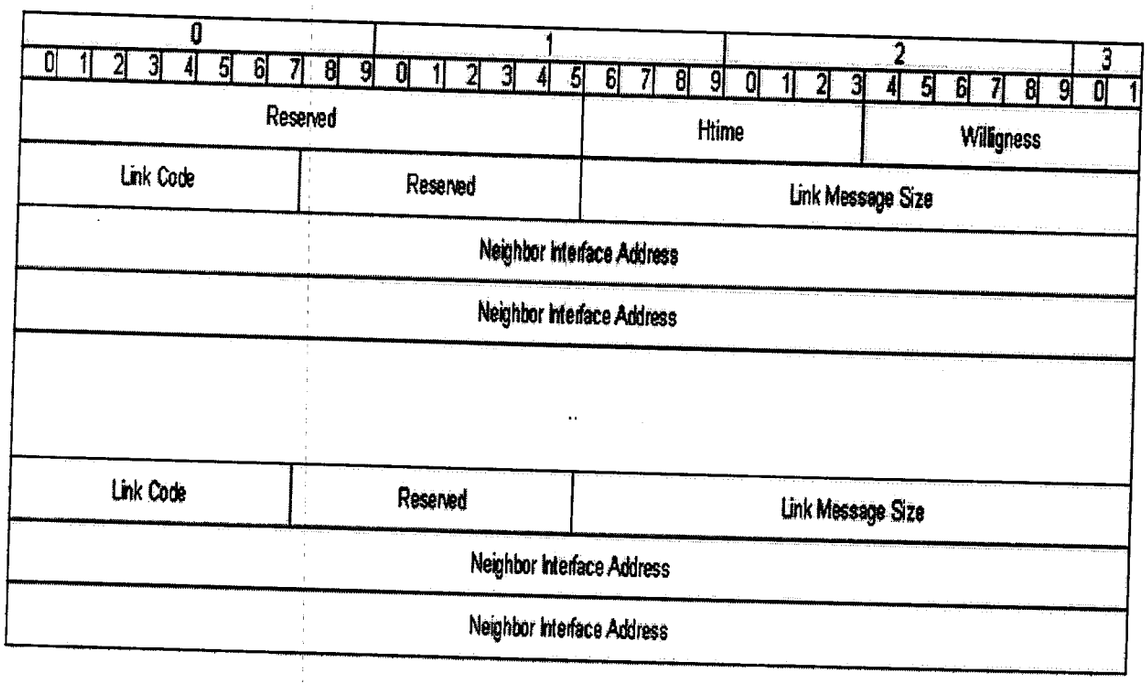


Figure III.5 :format du paquet

HELLO

Ceci est envoyé dans le paquet OLSR avec le "type de message" placé à HELLO_MESSAGE , avec le champ TTL égale a 1 (un) et Vtime réglé en conséquence à la valeur de NEIGHB_HOLD_TIME indiquée dans ce vient après[17].

- **Réservé**

Ce champ doit être placé à "0000000000000" pour être dans la conformité avec cette spécification. .

- **H time**

Ce champ indique l'intervalle d'émission employé par le nœud sur cette interface particulière, c.-à-d., le temps avant que la transmission du prochain hello message ne soit faite. L'intervalle d'émission est représenté par sa mantisse (les quatre bits les plus élevés de champ du Htime) et par son exposant (les quatre bits les plus bas de champ du Htime).

En d'autres termes :

HELLO émission intervalle=$C*(1+a/16)*2^{A}b$ [en secondes]

Avec :

-a : est le nombre entier représenté par les quatre bits les plus élevés du champ de Htime

-b : est le nombre entier représenté par les quatre bits les plus bas du champ de Htime.

-La valeur proposée du facteur de graduation C est déjà indiquée dans la partie précédente.

➢ **willingness**

Ce champ indique la bonne volonté d'un nœud de porter et expédier le trafic vers d'autres nœuds il est entre 0 et 7.

Un nœud avec la bonne volonté WILL_NEVER ne doit jamais être choisi comme MPR par n'importe quel nœud. Un nœud avec la bonne volonté WILL_ALWAYS doit toujours être choisi comme MPR. Par défaut, un nœud devrait annoncer une bonne volonté de WILL DEFAULT.

➢ **Link Code**

Ce champ indique des informations sur le lien entre l'interface de l'expéditeur et de la liste, suivante d'interfaces voisines. Il indique également des informations sur le statut du voisin.

➢ **Link Message Size**

La taille du message de lien, comptée en bytes et mesurée à partir du commencement du champ "Link Code" et jusqu'au prochain champ "Link Code" ou jusqu'à l'extrémité du message s'il n'existe pas un autre lien.

➢ **Neighbor Interface Address**

C'est l'adresse de l'interface du nœud voisin [16].

Code de lien comme type de lien et type de voisin

Cette partie indique seulement le traitement du lien code < 16.

Si l'élément de code de lien est inférieur ou égal à 15, alors il doit être interprété en tant que tenir deux champs différents, de deux bits chacun :

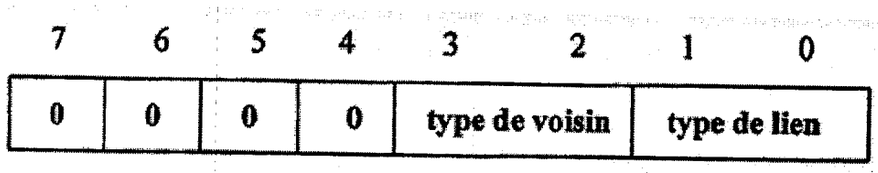


Figure III.6 :Link Code

Les types de lien sont 4 :

*UNSPEC_LINK - indiquant qu'aucune information spécifique sur les liens n'est fournie. ASYM_LINK - indiquant que les liens sont asymétriques (c.-à-d., l'interface voisine "est entendu").

*SYMJLINK - indiquant que les liens sont symétriques avec l'interface. LOST_LINK - indiquant que les liens ont été perdus

Les types de voisins" sont 3 :

*SYM_NEIGH - indiquant que les voisins ont au moins un lien symétrique avec ce nœud.

*MPR_NEIGH - indiquant que les voisins ont au moins un lien symétrique ET ont été choisis comme MPR par l'expéditeur.

*NOTNEIGH - indiquant que les nœuds ne sont plus ou n'ont pas les voisins symétriques
encore devenus.

III.7.2.HELLO Génération De Message

Ceci implique de transmettre l'ensemble de lien, l'ensemble de voisin et l'ensemble de MPR. En principe, un message hello sert à trois tâches indépendantes :

- ❖ sensation de lien
- ❖ détection voisine
- ❖ signalisation de choix de MPR

Les trois tâches sont toutes basées sur l'échange de l'information périodique dans un voisinage de nœuds, et atteignent l'objectif commun **"la découverte locale de la topologie".** Un message hello est donc produit en se basant sur les informations stockées dans les deux bases de données : **local link information base** et **Neighbor Hood Information Base**

III.7.3.La sélection des relais multipoint

Les relais multipoint sont un élément important du protocole OLSR. C'est sur la connaissance des voisins à deux sauts qu'ils sont déduits et c'est sur les MPR que repose la transmission des autres messages et donc la table de routage.

L'objectif de ces relais est d'arriver à faire communiquer l'ensemble des machines du réseau en faisant transiter les paquets de données par un nombre minimum de nœuds qui seront impliqués dans la communication. Les machines ne choisissent pas d'être relais multipoint.

Elles sont désignées par leurs voisins pour jouer ce rôle. Afin de bien en comprendre le fonctionnement, nous allons nous positionner sur un machine A et considérer deux listes. Soit M la liste des nœuds nécessitant un relais multipoints et R celle intégrant les MPR déjà sélectionnés. L'élection des MPR suit les étapes suivantes:

La première étape consiste à trouver les nœuds à deux sauts de A qui ne sont rattachés qu'a une seule machine située à un saut. Cette dernière notée B, permettant la liaison entre A et une machine C sera obligatoirement élue comme relais multipoint. Elle sera alors ajoutée à la liste R et l'ensemble des machines ou nœuds qu'elle pourra couvrir seront supprimés de la liste M des machines demandant un relais.

La deuxième et dernière étape ressemble à la première. On recherche les nœuds à un saut de A permettant de couvrir le plus de machines à deux sauts. Les machines choisies sont alors ajoutées à la liste R des MPR alors que les machines couvertes par ces relais sont supprimés de la liste M. Cette étape s'effectue en boucle jusqu'à ce que la liste M soit vide.

III.8.Decouverte de Topologie

Le lien sentant et pièce voisine de détection du protocole offre fondamentalement, à chaque nœud, une liste de voisins avec lesquels elle peut communiquer directement et, en combination avec la pièce de format et de expédition de paquet, un mécanisme optimisé d'inondation par MPRs. Basé sur ceci, l'information de topologie est diffusée dans le réseau.

Des itinéraires sont construits par des liens annoncés et des liens avec des voisins. Un nœud doit au moins disséminer des liens entre lui-même et les nœuds dans son ensemble de MPR-sélecteur, afin de fournir des informations suffisantes pour permettre le cheminement.

III.8.1.Format du Message TC (Topology Control Message)

Le format proposé d'un message TC est comme suit :

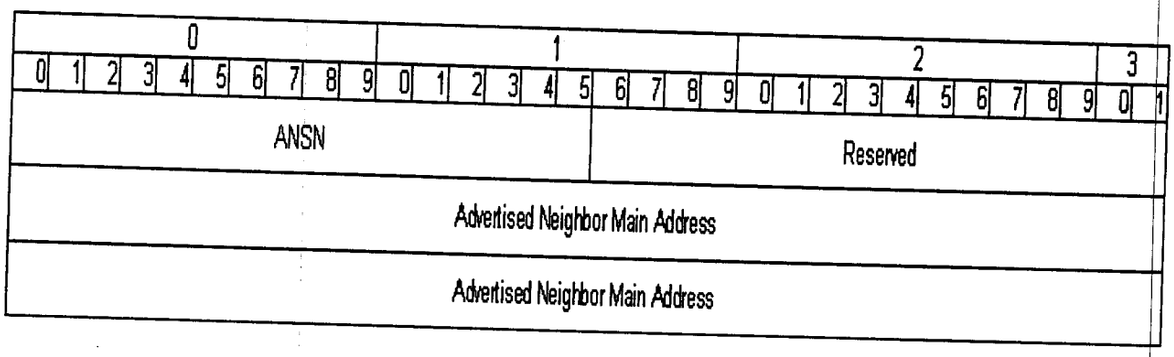


Figure III.7 : Format du message TC

Ceci est envoyé comme la partie DATA du format général de message avec le "type de message" placé à TC_message. Le Time to Live devrait être placé à 255 (valeur maximum) pour répandre le message dans le réseau.

Les messages TC permettent à chaque nœud, après analyse du message, de mettre à jour leur liste d'information sur la topologie du réseau. La liste intervient par la suite dans le calcul de la table de routage. Les messages TC ne sont créés que par des machines élues comme relais multipoint. Ils sont composés:

- D'un numéro de séquence permettant la gestion des messages périmés
- De la liste des voisins qui l'ont élu MPR. Cette liste peut être partielle à cause des limitations du réseau mais elle devra être émise de manière complète dans un intervalle de temps fixe.

❖ Nombre de séquence du Voisin Annoncé (ANSN)

Un nombre de séquence est associé à l'ensemble annoncé de voisin. Chaque fois qu'un nœud détecte un changement de son ensemble annoncé de voisin, il incréments ce nombre d'ordre. Ce nombre est introduit dans le champ d'ANSN du message TC pour maintenir l'information la plus récente. Quand un nœud reçoit un message TC, il peut décider en basant sur le nombre d'ordre voisin annoncé, si les informations reçues sur les voisins annoncés du nœud générateur sont plus récentes des précédentes.

❖ Réservé

Ce champ est réservé, et doit être placé à "0000000000000000".

❖ **Adresse Principale Voisine Annoncée**

Ce champ contient l'adresse principale d'un nœud voisin. Toutes les adresses principales des voisins annoncés du nœud générateur sont mises dans le message TC. Si la taille permise maximum du message (comme imposé par le réseau) est atteinte tandis qu'ils restent des adresses voisines annoncées qui n'ont pas été insérées dans le message TC, alors plus de messages TC seront produits jusqu'à ce que l'ensemble annoncé entier de voisin sera envoyé.

III.8.2.Ensemble Annoncé De Voisin

Un message TC est envoyé par un nœud dans le réseau pour déclarer un ensemble de liens, appelé l'ensemble de lien annoncé qui doit inclure au moins les liens à tous les nœuds de son ensemble de sélecteur de MPR, c.-à-d., les voisins qui ont choisi le nœud d'expéditeur comme MPR.

Le nombre d'ordre (ANSN) lié à l'ensemble annoncé de voisin est également envoyé avec la liste. Le nombre d'ANSN doit être incrémenté quand des liens sont enlevés de l'ensemble annoncé de voisin; le nombre d'ANSN devrait être incrémenté quand des liens sont ajoutés à l'ensemble annoncé de voisin.

III.8.3.Génération De Message TC

Afin d'établir la base de données de topologie, chaque nœud, qui a été choisi comme MPR, annonce des messages de commande de topologie. Des messages TC sont inondés à tous les nœuds dans le réseau et tirent profit de MPRs. MPRs permettent une meilleure optimisation dans la distribution de l'information de topologie.

La liste d'adresses peut être partielle dans chaque message TC (par exemple, en raison des limitations de taille de message, imposées par le réseau), mais l'analyse de tous les messages TC décrivant l'ensemble de lien annoncé d'un nœud doit être complète au cours d'une certaine période (TC_INTERVAL).

L'information diffusée dans le réseau par ces messages TC aide chaque nœud pour calculer sa table de routage

Quand l'ensemble de lien annoncé d'un nœud devient vide, ce nœud immobile envoie les messages TC (vides) pendant une durée égale à la "période de validité" (typiquement, ce sera égal à TOP_HOLD_TIME) de ses messages

TC précédemment émis, afin d'infirmer les messages TC précédents. Il devrait alors cesser l'envoi des messages TC jusqu'à ce qu'un certain nœud soit inséré dans son ensemble de lien annoncé.

Expédition Des Messages TC

Les messages TC sont émis et retransmis par les MPRs afin de diffuser les messages dans le réseau entier.

III.9.Calcule de la Table de Routage

Chaque nœud maintient une table de routage qui lui permet de relayer les données destinées aux autres nœuds dans le réseau. La table de routage est basée sur l'information contenue dans la base locale de l'information de lien et l'ensemble de topologie. Par conséquent, si un quelconque de ces ensembles est changé, la table de routage est recalculée pour mettre à jour les informations d'itinéraire sur chaque destination dans le réseau. Les entrées d'itinéraire sont enregistrées dans la table de routage dans le format suivant :

Chaque entrée dans la table se compose de R_dest_addr, R_next_addr, R_dist, et de R_iface_addr. Une telle entrée indique qu'on estime que le nœud identifié par R_dest_addr est des sauts de R_dist loin du nœud local, que le nœud voisin symétrique avec l'adresse R_next_addr d'interface est le prochain nœud (saut) dans l'itinéraire à R_dest_addr, et que ce nœud voisin symétrique est accessible par l'interface locale avec l'adresse R_iface_addr. Des entrées sont enregistrées dans la table de routage pour chaque destination dans le réseau pour Lequel un itinéraire est connu. Toutes les destinations, pour lesquelles un itinéraire est cassé ou seulement partiellement connu, ne sont pas enregistrées dans la table [16].

La table de routage est mise à jour quand un changement est détecté dans les bases suivantes :

- l'ensemble de lien,
- l'ensemble de voisin,
- l'ensemble du voisin 2-hop,
- l'ensemble de topologie

III.10.Valeurs proposée pour les constantes

Cette partie donne les valeurs proposées pour les constantes employées dans la description du protocole.

➢ **Intervalles d'émission**

HELLO_INTERVAL = 2 secondes REFRESHJNTERVAL = 2 secondes TCINTERVAL = 5 secondes

➢ **Le Temps**

NEIGHBHOLDTIME = 3 x REFRESHJNTERVAL TOP_HOLD_TIME = 3 x TCJNTERVAL DUP HOLD TIME = 30 seconds

Le Vtime dans l'en-tête du message, et le Htime dans le message hello sont les champs qui tiennent des informations sur les valeurs ci-dessus. En d'autres termes : Valeur = C*(l+a/16)*2^{A}b [en secondes]

Où:

a : le nombre entier représenté par les quatre bits les plus élevés du champ ; *h :* le nombre entier a représenté par les quatre bite les plus bas du champ.

- **Types De Message**

HELLO_MESSAGE = 1 TC_MESSAGE = 2

- **Types De Lien**

UNSPECJLINK = 0 ASYM_LINK = 1 SYM_LINK = 2 LOST_LINK = 3

- **Types Voisins**

NOT_NEIGH = 0 SYMJSTEIGH = 1 MPR NEIGH = 2

- **Bonne volonté (willingness)**

WILL_NEVER = 0 WILLLOW = 1 WILLDEFAULT = 3 WILL_HIGH = 6 WILL_ALWAYS = 7

La bonne volonté d'un nœud peut être placée à n'importe quelle valeur de nombre entier de 0 à 7, et indique comment le disposé d'un nœud doit être le trafic de expédition au nom d'autres nœuds. Les nœuds, par défaut, auront une bonne volonté WILL_DEFAULT. WILLNEVER indique un nœud qui ne souhaite pas porter le trafic pour d'autres nœuds, par exemple dû aux contraintes de ressource (comme être bas sur la batterie). WILL_ALWAYS indique qu'un nœud toujours devrait être choisi pour porter le trafic au nom d'autres nœuds, par exemple en raison de l'abondance de ressource (comme l'alimentation d'énergie permanente, les interfaces de capacité élevée à d'autres nœuds).

Un nœud peut dynamiquement changer sa bonne volonté pendant que ses conditions changent.

Une application possible, par exemple, serait pour un nœud, relié à une alimentation d'énergie permanente et aux batteries entièrement chargées, pour annoncer une bonne volonté de WILL_ALWAYS. En étant démonté de l'alimentation d'énergie permanente (par exemple, un PDA étant pris hors de son berceau de remplissage), une bonne volonté de LL_DEFAULT est annoncée. Car la capacité de batterie est vidangée, la bonne volonté serait encore réduite. D'abord à la valeur intermédiaire entre WILL_DEFAULT et WILL_LOW, puis à WILL_LOW et finalement à WILL_NEVER, quand la capacité de batterie du nœud ne soutient plus le trafic étranger.

III.11.conclusion

Pour maintenir à jour toutes les informations nécessaires au choix des relais multipoints et le calcul de la table de routage, les nœuds OLSR ont besoin de s'échanger des informations périodiquement.

Pour s'informer du proche voisinage, les nœuds OLSR envoient périodiquement des messages dits HELLO contenant la liste de leurs voisins. Ces messages permettent à chacun de choisir son ensemble de relais multipoints.

Itemize Le deuxième type de message d'OLSR, sont les messages TC (*Topology Control*). Par ce message les sous-ensembles de voisinage que constituent les relais multipoints sont déclarés périodiquement dans le réseau

Ils sont diffusés en utilisant une diffusion optimisée par relais multipoints. Ces informations offrent une carte de réseau contenant tous les nœuds et un ensemble partiel des liens, mais suffisant pour la construction la table de routage.

La table de routage est calculée par chacun des nœuds et le routage des données s'effectue saut par saut sans l'intervention d'OLSR dont son rôle s'arrête à la mise à jour de la table de routage de la pile IP.

En effet, nous avons prendre la sécurité de protocole OLSR, et les attaques contre le protocole OLSR. Cette dernière sera traitée en détail dans le quatrième chapitre.

Chapitre IV

La sécurité du protocole OLSR

IV.1.Introduction

Durant les dernières années, le besoin à plus de mobilité et à pouvoir accéder à des données partagées ou à s'échanger de l'information à tout moment, en utilisant des dispositifs mobiles (téléphones portables, PDA, PC portables, ...) a rendu très répandu la notion de réseau sans infrastructure, ou réseaux Ad hoc.

Les réseaux Ad hoc ont une architecture d'un graphe arbitraire dans lequel, un ensemble de nœuds sans fils forment temporairement un réseau sans l'aide d'une infrastructure ou une administration centralisée quelconque. , un réseau mobile Ad hoc est un système autonome de routeurs mobiles connectés par des liens sans fils. Les réseaux Ad hoc ont plusieurs caractéristiques: une topologie dynamique, l'absence d'infrastructure, la capacité variable des liens et une source d'énergie limitée. A partir de ces caractéristiques, on peut déduire les problèmes et difficultés que peut poser ce type de réseaux : les contraintes de bande passante, le coût élevé, les contraintes d'énergie, la sécurité et la non compatibilité entre différentes normes en sont quelques uns.

Les réseaux Ad hoc commencent à s'imposer fortement dans différents domaines d'applications. C'est dans le domaine du routage qu'il y a eu beaucoup de travaux de recherche. Il reste beaucoup d'autres domaines à explorer et de problèmes à résoudre ou pour lesquels il faut améliorer les solutions déjà existantes. Les problèmes de QoS, les problèmes de batteries ou encore ceux de la sécurité en font partie.

Dans les réseaux Ad hoc, la sécurité dépend de plusieurs paramètres (authentification, confidentialité, intégrité, non répudiation et disponibilité) et concerne deux aspects, la sécurité du routage et la sécurité des données. Ces deux aspects comportent certaines vulnérabilités et sont exposés à plusieurs attaques.

IV.2.Fonction et données à protéger

Pour cerner le problème de la sécurité, il faut tout d'abord déterminer les ressources sensibles qu'on doit protéger. Comme les réseaux fixes, un réseau Ad Hoc doit garantir la validité et l'intégrité des informations transmises.

Chaque nœud d'un réseau Ad Hoc se comporte comme un routeur. Ainsi, il participe dans la découverte des routes et échange des informations de routage avec les autres nœuds du réseau. Supposons qu'un nœud malicieux réussit à introduire des informations de routage invalides alors tout le réseau tombe en panne (les nœuds n'arrivent pas à communiquer). Le routage est donc une fonction sensible qu'il faut protéger pour garantir la disponibilité du réseau.

Les informations relatives au routage comme les nœuds accessibles et les métriques associées aux routes, les informations relatives aux mécanismes de configuration et les informations personnelles des utilisateurs sont considérées comme des données sensibles qu'il faut protéger [18].

IV.3.Service de sécurité

Les réseaux Ad Hoc doivent satisfaire les services de sécurité suivants :

- ***Contrôle d'accès*** : empêcher les nœuds étrangers d'accéder au réseau. Le contrôle d'accès donne aux nœuds légitimes un moyen de détecter les messages provenant de sources externes au réseau.
- ***Authentification*** : s'assurer de l'identité des entités en cours de communication Avec l'authentification, le destinataire sera sûr que le message provient de la source prétendue.
- ***Confidentialité*** : assurer que l'information ne peut pas être interprétée par des autorisés. Les informations de routage doivent aussi, dans certains cas, rester secrètes.
- ***Intégrité*** : assurer que la modification des données transmises sera détectée. On utilise souvent les fonctions de hachage pour assurer l'intégrité.
- ***Non répudiation*** : empêcher un nœud de nier l'envoi ou bien la réception d'un message.
- ***Fraîcheur*** : garantir que les données présentes échangées sur le réseau sont viables.

Ce service permet de lutter contre la réinjection d'anciens messages interceptés par un attaquant.

- ***Disponibilité*** : assurer la présence des services du réseau même en présence d'attaques de déni de service. Ces attaques peuvent se présenter au niveau de différentes couches d'un réseau Ad Hoc. La disponibilité donne aussi une assurance sur la réactivité et le temps de réponse du réseau [18].

IV.4.Vulnérabilités

Les réseaux Ad Hoc présentent quelques faiblesses. Certaines faiblesses sont liées à la technologie sans fil, d'autres aux caractéristiques de ces réseaux.

La première vulnérabilité de ces réseaux est liée à la technologie sans fil sous-jacente. En effet l'utilisation d'un canal radio favorise l'écoute et la perturbation des messages échangés par tout nœud possédant le récepteur adéquat même s'il se trouve dans un lieu public, à l'extérieur du bâtiment où se déroulent les échanges.

Les nœuds sont aussi des points de vulnérabilité du réseau. En effet, un attaquant peut compromettre un terminal laissé sans surveillance.

L'absence d'infrastructure fixe est une autre faiblesse des réseaux Ad Hoc car elle rend impossible l'utilisation d'une entité centrale pour la gestion des accès aux ressources du réseau.

De même, la capacité limitée des nœuds en puissance de calcul et énergie consommée empêche l'utilisation des mécanismes cryptographiques résistants comme la cryptographie à clé publique [18].

IV.5.les attaque possible dans les protocoles de routage

Une première classification des attaques consiste à distinguer les attaques passives des attaques actives.

> ***Les attaques passives*** se limitent à l'écoute et l'analyse du trafic échangé. Ce type d'attaques est plus facile à réaliser (il suffit de posséder le récepteur adéquat) et il est difficile à détecter puisque l'intrus n'apporte aucune modification sur les informations échangées. L'intention de l'intrus peut être la connaissance des informations confidentielles des utilisateurs ou bien la connaissance des nœuds importants dans le réseau, en analysant les informations de routage, pour se préparer à une attaque active.

> Dans les ***attaques actives***, un intrus tente de supprimer ou modifier les messages transmis sur le réseau. Il peut aussi injecter son propre trafic ou rejouer d'anciens messages pour perturber le fonctionnement du réseau ou provoquer un déni de service [18].

> Parmi les attaques actives les plus connues, on peut citer :

- ***Relais sélectif de paquets (Sélective forwarding)*** : Un nœud décide de ne pas transmettre les données de certains nœuds. La raison peut être aussi bien d'ordre énergétique, que liée à une attaque.

- ***Attaque du trou noir (blackhole):*** Un nœud falsifie les informations de routage pour forcer le passage des données par lui-même. Sa seule mission est ensuite de ne rien transférer, créant ainsi une sorte de puits ou « trou noir » dans le réseau.

- ***Attaque du trou de ver (wormhole)*** : Cette variante du trou noir consiste à réinjecter les paquets absorbés en un autre point (souvent distant) du réseau. Pour des distances plus longues que la couverture normale d'une transmission sans fil d'un hop, un attaquant peut s'arranger pour faire arriver ses paquets plus rapidement que par une route multi-hops. Il suffit pour lui d'utiliser un réseau externe câblé ou un transfert sans fil directionnel à forte puissance.

> ***Attaque de l'identité multiple*** : Cette attaque porte le nom anglais de Sybil attack. Un nœud se fait passer pour plusieurs nœuds potentiellement distants, créant des incohérences dans les tables de routage des nœuds voisins.

> ***Attaque par chantage*** : Elle est connue sous le nom anglais de Black mail attack. Un nœud malicieux fait annoncer qu'un autre nœud légitime est malicieux pour éliminer ce dernier du réseau. Si le nœud malicieux arrive à attaquer un nombre important de nœuds, il pourra perturber le fonctionnement du réseau.

> ***Attaque par l'inondation de HELLO*** : La plus simple attaque pour un intrus consiste à envoyer un flot de tels messages pour inonder le réseau et empêcher d'autres messages d'être échangés. De plus, s'il parvient à émettre à une portée suffisante, des nœuds distants vont ajouter l'intrus comme nœud voisin dans leurs routes et fausser ainsi complètement le routage de l'information dans le réseau.

> ***Brouillage radio*** : II consiste à perturber le canal radio en envoyant des informations inutiles sur la bande de fréquences utilisées. Ce brouillage peut être temporaire, intermittent ou permanent.

De même, son champ d'action doit être pris en compte ; son effet est-il limité à quelques nœuds ou est-il suffisamment puissant pour bloquer le réseau tout entier

- ***Privation de mise en veille*** : Elle a pour but de consommer toutes les ressources de la victime en l'obligeant à effectuer des calculs ou à recevoir ou transmettre des données inutilement.

IV.6.Les attaques possible dans les protocoles de routage

Dans cette partie, nous énumérons les attaques possibles qui ciblent les protocoles de routage. Ce type d'attaque peut perturber le fonctionnement du réseau. On peut aussi classer ces attaques en deux catégories :

> Les **attaques** passives dans lesquelles l'intrus intercepte et analyse le trafic pour déterminer les relations entre les nœuds et éventuellement déterminer les nœuds importants dans le fonctionnement du réseau. Ces informations peuvent être une préparation pour lancer une attaque active. Par exemple une attaque par déni de service ciblant les nœuds importants peut faire tomber le réseau (mettre en disfonctionnement).

> Les attaques actives dans lesquelles l'intrus tente de perturber le fonctionnement du réseau en supprimant, en modifiant, en fabriquant des paquets ou en rejouant d'anciens paquets.

IV.6.1.Attaques par suppression de paquets

Dans ce type d'attaque, l'intrus supprime tous ou certains paquets. On peut trouver deux types :

- **Trou noir (Black holes)** : L'attaquant supprime tous les paquets (contrôle et donnée).
- **Trou gris (Gray holes)** : C'est un cas particulier du trou noir dans lequel l'attaquant supprime les paquets de données et transmet ceux de contrôle.

IV.6.2.Attaques par modification des informations de routage

En absence de contrôle d'intégrité sur les messages transmis, un nœud malicieux peut rediriger le trafic vers lui ou causer un déni de service, simplement par la modification de certains champs des paquets de contrôle utilisés par les protocoles de routage [18].

IV.6.3.Attaques par usurpation d'identité (Spoofing)

Un nœud malicieux change son adresse IP ou son adresse MAC afin de se faire passer pour un autre nœud légitime du réseau. L'intrus ensuite peut lancer ses attaques avec l'identité de ce nœud.

IV.7.Attaque contre le protocole OLSR

Nous discutons maintenant des risques de sécurité dans OLSR. Le but n'est pas de remarquer les failles dans OLSR, car il n'a pas été conçu comme protocole sécurisé, mais de donner des exemples des risques que courent tous les protocoles à état de liens, comme OSPF [19].

➢ ***Génération incorrecte du trafic***

Un nœud malveillant X peut envoyer des messages HELLO ayant une fausse origine F. En conséquence, d'autres nœuds pourraient, en se trompant, déclarer être voisins de F à travers leurs messages HELLO et TC. En outre, le nœud X choisit ses MPR parmi ses voisins avec l'identité de F ; de ce fait, ces MPR vont déclarer qu'ils sont voisins de F. L'effet de cette attaque se traduit par des conflits des routes vers F, avec perte de connectivité [19]. La signalisation **(link spoofing)** d'une relation de voisinage avec des nœuds qui en fait ne sont pas des voisins. Un nœud X déclarant faussement un lien avec un nœud éloigné obtient un faux voisinage à deux sauts pour ses voisins, et donc une mauvaise sélection des MPR. Le nœud X peut aussi signaler un ensemble incomplet de voisins; les voisins ignorés pourraient éventuellement se trouver coupés du reste du réseau.

Si le nœud X envoie un TC ayant pour origine F et déclarant A comme voisin, le nœud A mémorisera faussement une relation de voisinage entre F et A. Des messages TC qui contiennent des faux liens ont aussi cet effet néfaste, et peuvent perturber la topologie du réseau. Un nœud malveillant peut aussi générer des TC avec une fausse origine A et un ANSN (Advertised Neighbor Séquence Number) plus élevé que celui du dernier TC envoyé par A. Tous les nœuds ignoreront donc tout message TC ultérieur de la part de A, parce qu'il porte un ANSN avec une valeur inférieure. Nous appelons ceci une attaque ANSN.

➢ ***Relayage incorrect du trafic***

Un dégât important peut être apporté au réseau, en termes de connectivité, si les messages TC ne sont pas relayés (blackhole attack).

Concernant les attaques de rejeu, un TC ne peut pas être rejoué à moins d'augmenter son ANSN, engendrant ainsi une attaque ANSN.

Un wormhole peut être créé par un nœud intrus X en faisant suivre les messages de A vers F et vice-versa. L'attaque commence à être efficace quand A et F sont unis par un lien symétrique; jusqu'à ce moment là, tout message TC acheminé à travers le wormhole est refusé soit par A soit par F, parce que les spécifications d'OLSR imposent que ces messages soient rejetés si le nœud émetteur n'est pas un voisin symétrique [19].

Un adversaire peut exploiter la règle d'OLSR qui spécifie qu'un nœud recevant un message en inondation MPR ne retransmet plus le message si l'envoyeur est son MPR selector. Cette **attaque MPR** est produite par une retransmission illicite du message effectuée par l'attaquant

V.8.Exemple d'attaque sur le protocole OLSR

IV.8.1.Insertion de faux messages HELLO

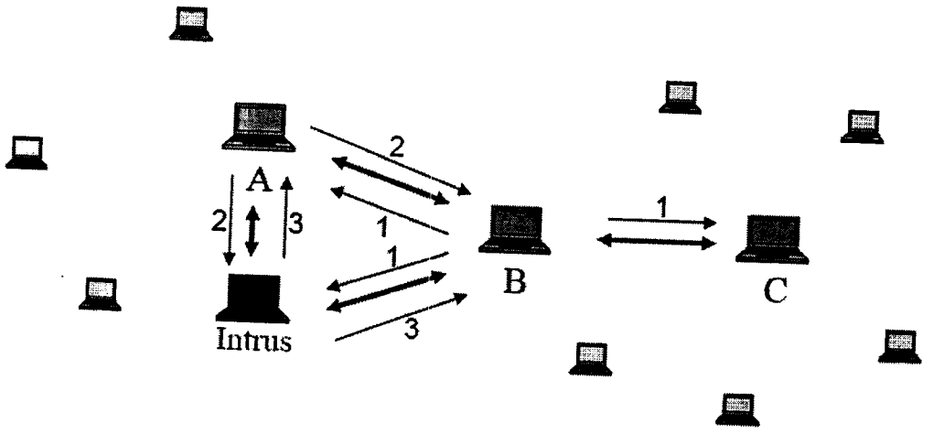


Figure IV-1 : Insertion de faux messages HEllo

B est MPR de A. C. est à 2 hops de A

1. Envoi de messages Hello par B
2. Envoi de messages Hello par A
3. Insertion d'un message Hello par l'Intrus annonçant à A, B, C et X un lien symétrique

> Conséquences :

- Sélection de l'Intrus comme MPR par A et B
- Le trafic de A vers C passera par l'Intrus.

IV.8.2.insertion de faux messages TC

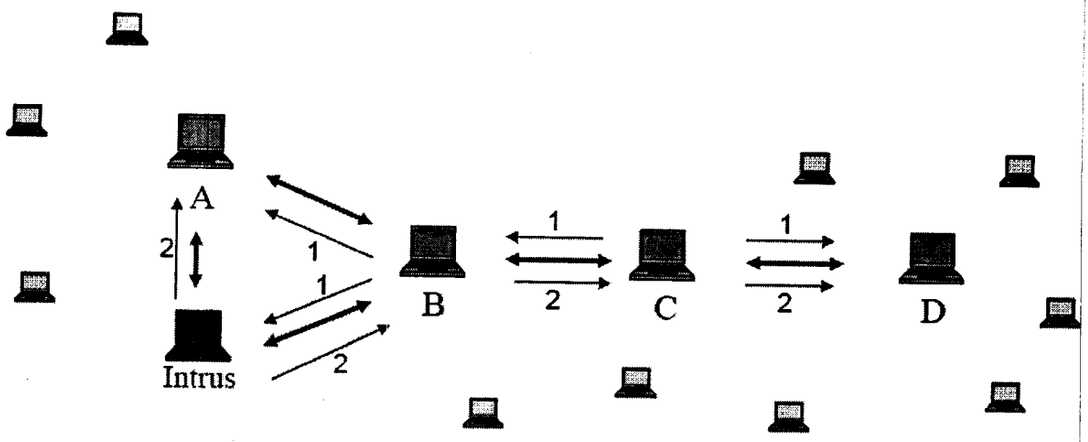


Figure IV-2 : Insertion de faux messages TC

A possède une route vers D à 3 hops en passant par B

1. Envoi d'un message TC par C : l'intrus identifie D à trois hops
2. Envoi d'un message TC par l'Intrus annonçant D faisant partie de son MS set

> Conséquences :

- A arrête d'envoyer du trafic vers D en passant par B.
- A envoie son trafic vers D en passant par l'Intrus.

► D ne réagit pas aux fausses infos annoncées dans le TC qu'il reçoit

IV.8.3.La modification

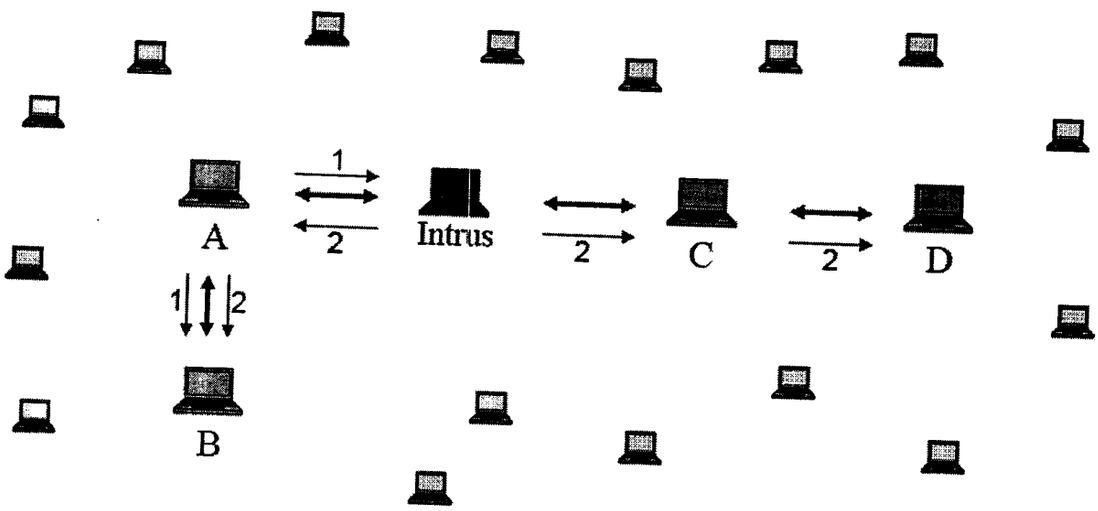


Figure IV-3 : la modification

1. A envoie un message TC avec Message Séquence Number = x

2. L'intrus transfère le message TC reçu avec un Message Séquence Number modifié en x+i

Conséquences :

• C et D arrêtent de traiter et de transférer les messages TC provenant de A ayant un Message Séquence Number < x+i

IV.8.4.L'usurpation d'identité

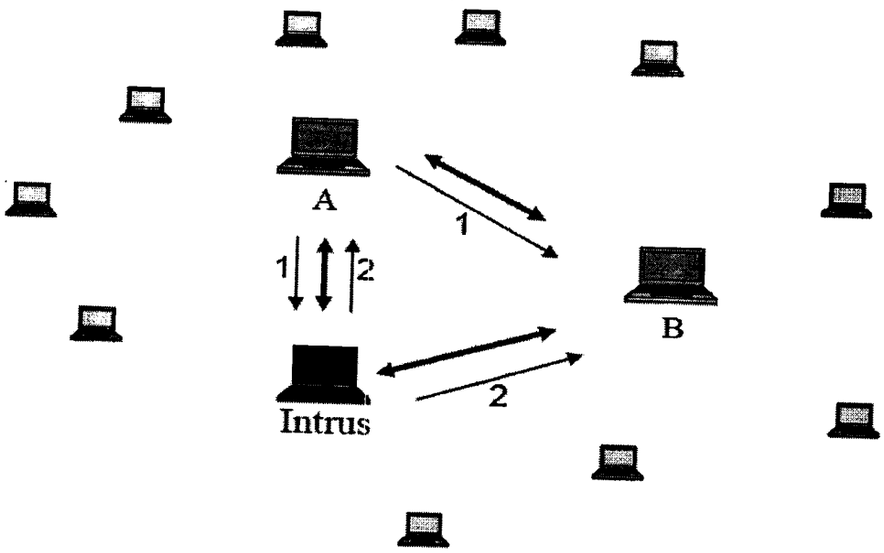


Figure IV-4 : L'usurpation d'identité

1. A envoie un message Hello ; l'Intrus identifie B comme voisin de A

2. Après réception du message Hello de A, l'Intrus fabrique un message Hello en se faisant passer pour A, et annonçant à B que le lien est perdu

Conséquence :

• B change l'état de son lien avec A à « heard »

IV.9.La sécurité d'OLSR

IV.9.1.Travaux effectués

Plusieurs approches et solutions ont été proposées pour sécuriser les réseaux Ad hoc. Chacune se base sur un raisonnement différent suivant le type d'application, l'extension du réseau, la moyenne du nombre de nœuds ainsi que les aspects de sécurité pris en priorité (confidentialité, authenticité,...)- On trouve par exemple IPsec, WEP (Wireless Equivalent Privacy),

Aussi que le domaine important de la sécurité des réseaux Ad hoc. On peut classer les approches existantes en quatre catégories:

- Modèles de confiance
- Modèles de gestion de clés
- Sécurisation des protocoles de routage
- Systèmes de détection d'intrusion

Dans la suite de ce chapitre on s'intéressera uniquement à la sécurisation du protocole OLSR et aux systèmes de détection d'intrusion. On supposera l'existence préalable d'un système de gestion des clés pour le réseau Ad hoc.

IV.9.2.Sécurisation d'OLSR par un message SIGNATURE

Nous allons décrire une approche de sécurisation d'OLSR, qui fait appel à l'ajout d'une signature aux messages de contrôle. Un digest, généré au moyen d'une clé symétrique partagée, peut aussi bien être utilisé à la place de la signature.

La signature est calculée sur le corps et l'entête du message, et est distribuée sous la forme d'un type spécial de message, appelé SIGNATURE. Un message SIGNATURE est généré et envoyé avec tout autre message de contrôle (HELLO, TC). Il n'est pas possible de signer un paquet entier parce qu'il peut contenir des HELLO, qui ne sont pas relayés, et donc la signature du paquet ne serait plus valable au delà du premier saut. Une solution serait celle de contrôler la signature saut par saut; toutefois, comme les messages sont relayés par inondation MPR, tout nœud qui a relayé un message incorrect pourrait en être l'émetteur, tandis qu'une authentification par message permet de déterminer aisément l'origine des fausses informations. On identifie sans ambiguïté à quel message appartient une signature car les deux doivent se trouver dans un même paquet OLSR et sont consécutifs. Dans une version précédente, le couplage était identifié grâce au Numéro de Séquence (MSN) du message de contrôle en question et à un champ homologue dans le message de signature; cela permettait d'envoyer les messages dans un ordre quelconque, et même dans des paquets différents.

Si la taille du paquet dépasse le MTU, le message de contrôle est fragmenté et un message SIGNATURE est associé à chaque fragment. Le message SIGNATURE contient aussi une estampille temporelle, obtenue de l'horloge interne du nœud, pour éviter les attaques de rejeu; la synchronisation des horloges ne nécessite pas d'être très précise, puisque les messages qui seraient des doublons peuvent être reconnus aussi par leur Numéro de Séquence (qui est enregistré dans le Duplicate Set).

L'implantation a recours à la cryptographie asymétrique et une CA hors ligne pour assigner une paire de clés à chaque nœud participant; chaque nœud diffuse ensuite sa clé publique aux autres nœuds.

La signature n'inclut pas les champs TTL et de compte de sauts (dans l'entête du message). Cela est dû au fait que ces deux champs sont modifiés à chaque saut du message, ce qui interférerait avec la vérification de la signature.

Cette architecture de sécurité n'est pas inter opérable avec OLSR standard. En effet, un

nœud dans lequel tourne OLSR sécurisé n'accepterait pas des HELLO non signés de la part des nœuds OLSR standard; en conséquence il ne pourrait pas y avoir de lien symétrique entre les deux, et donc aucune sélection des MPR qui est le mécanisme principal pour la diffusion des messages dans OLSR

IV.9.3.Estampillage temporel

Comme il a été dit précédemment, un problème des systèmes distribués est qu'il est possible de rejouer des messages même si le contrôle des signatures est mis en place. Pour prévenir ce genre d'attaques, on a ajouté aux messages une estampille temporelle ou un *nonce,* qui est incluse dans le calcul de la signature. Dans OLSR, le protocole de routage peut déterminer quelle information est la plus récente en examinant le MSN (Message Séquence Number) et

le ANSN (Advertised Neighbor Séquence Number) des messages; ce mécanisme est toutefois suffisant pour le fonctionnement de base mais pas pour une sécurité complète, car les deux champs sont codés sur 16 bits et les débordements avec remise à zéro peuvent être fréquents.

Pour tout message émis par un nœud, une estampille temporelle est incluse.

Un nœud récepteur vérifie la validité de l'estampille temporelle, en vérifiant que sa valeur ne s'écarte de la valeur de son horloge de plus d'une petite constante.

Pour ce qui concerne le contrôle temporel des messages, il existe différentes options:

_ Si une protection contre les attaques de rejeu n'est pas requise, le champ relatif à l'estampillage temporel peut être simplement ignoré.

_ Une solution simple pour générer des est ampille temporelles serait celle d'avoir une horloge, suffisamment précise et avec un faible dérive, embarquée dans chaque nœud; cette solution peut être implantée sous forme d'une horloge au quartz ou atomique, ou bien d'un dispositif GPS pour la transmission du temps. Dans les ordinateurs de bureau, cette horloge est l'horloge interne ou du BIOS, présentant une dérive d'environ 1 seconde par jour qui toutefois peut être réduite au moyen de corrections de la fonction du temps.

_ Une implantation pour des simples estampilles temporelles consiste à écrire la valeur de l'horloge dans tout message envoyé (et signé), tandis que les nœuds récepteurs maintiennent une liste des plus grandes valeurs d'horloge reçues dans un message, pour chaque nœud émetteur.

Un message, de la part d'un certain nœud, est accepté s'il porte une valeur d'horloge supérieure à la valeur déjà enregistrée pour ce nœud; dans ce cas, la valeur enregistrée est mise à jour. Ce système présente des problèmes de synchronisation si les communications entre les

nœuds sont coupées pendant une certaine période.

_ La solution la plus sûre consiste en une synchronisation des horloges des nœuds, solution qui toutefois fait surgir un problème d'inter blocage: les estampilles temporelles sont utilisées pour l'authentification, mais une synchronisation sécurisée des horloges demande aussi une authentification.

IV.9.4.Modifications du protocole OLSR standard

Au moment de la création d'un message de contrôle, un nœud doit générer aussi un message SIGNATURE et y écrire les champs relatifs au temps et à la signature.

Un nœud recevant ces messages doit retenir la SIGNATURE et vérifier si le message de contrôle est acceptable du point de vue de la signature et de son temps de création; si ces vérifications réussissent, le message de contrôle est traité. Un message de contrôle ou de SIGNATURE non valable est effacé de la Duplicat Table, pour éviter qu'un adversaire remplisse la Duplicate Table d'un nœud avec des messages non valables et empêche le nœud de traiter des messages valables qui ont le même Numéro de Séquence. Le Duplicate Set est modifié avec un nouveau champ qui prend en compte l'estampille temporelle.

Le message de SIGNATURE est encapsulé et transmis comme la partie de données dans le format standard de paquet d'OLSR.

Le type de message champ est placé à la valeur de constante de SIGNATURE ; cette valeur peut également inclure des informations sur les primitifs et les clés cryptographiques à employer. Les champs de Time to Live et de Vtime sont placés aux valeurs du temps des champs TTL et de Vtime du message auquel la signature est associée. Les autres champs de l'en-tête de message sont placés comme d'habitude.

➢ ***Format du message de signature : Version prolongée*** :

Une vieille version du message de SIGNATURE est montrée sur la figure IV-5.

> le message porte un champ de MSN Referrer afin d'identifier la relation entre le générateur du message et son message de SIGNATURE.

> Le SignMethod. indique quelle méthode, parmi un ensemble prédéfini, est employée pour produire de la signature. Ceci inclut des informations sur des clés, fonctions cryptographiques, et algorithmes d'horodateur.

> Le champ réservé est employé pour le remplissage, pour faire tout le bit des champs 32 aligné. Il est placé à 0 et réservé pour le futur usage.

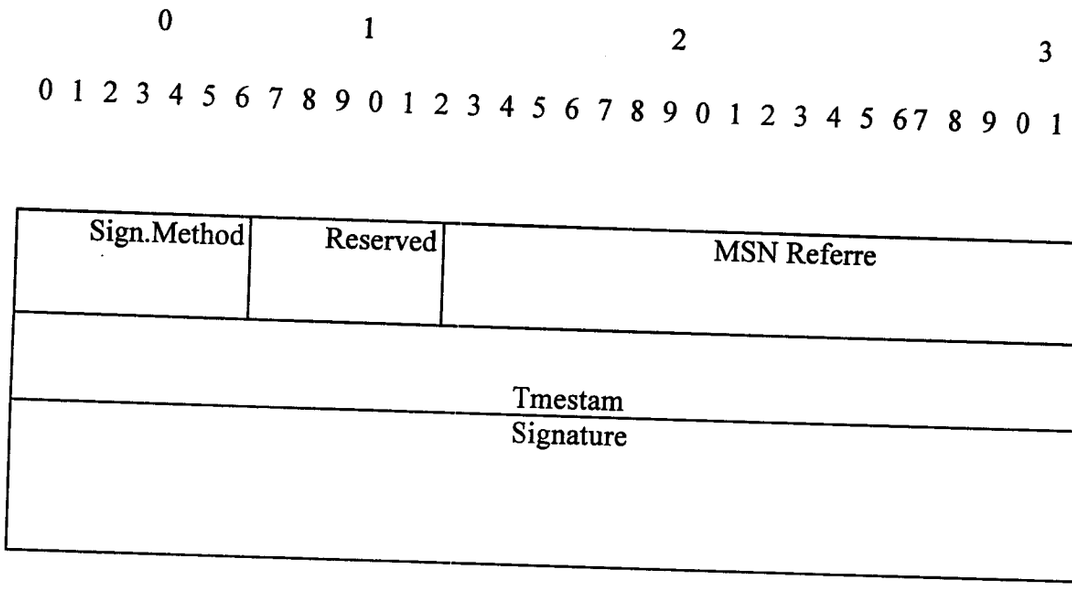


Figure IV-5: Format de la version prolongée du message de signature

Les champs d'horodateur (Timestamp) et de signature sont les mêmes que dans la version réelle du message.

➢ ***Version simplifiée***

Le format réel d'un message de SIGNATURE est indiqué sur la figure IV-6.

Le champ d'horodateur contient l'horodateur lui-même, mesuré en secondes. C'est l'horodateur du message de SIGNATURE et du message associé de commande. Pour des raisons de compatibilité, l'horodateur est 32 bits longs

Le temps courant est obtenu à partir de l'horloge interne du BIOS du nœud. L'horloge du BIOS à une dérive linéaire d'environ 1 sec/jour, qui peut donc être corrigée par l'intermédiaire d'un algorithme. Le champ de signature contient la signature, calculée sur des champs suivants :

> L'en-tête de message (80 bits) du message de commande, à l'exclusion du temps TTL et le compteur de sauts

Ces champs ne sont pas considérés dans le calcul de la signature parce qu'ils sont modifiés tandis que le message est dedans passage (le Time to Live est diminué de 1 et le compteur de sauts est augmenté par 1 à chaque saut) ;

> Le message de commande (DATA qui a une taille variable) ;

> Le champ d'horodateur (32 bits).

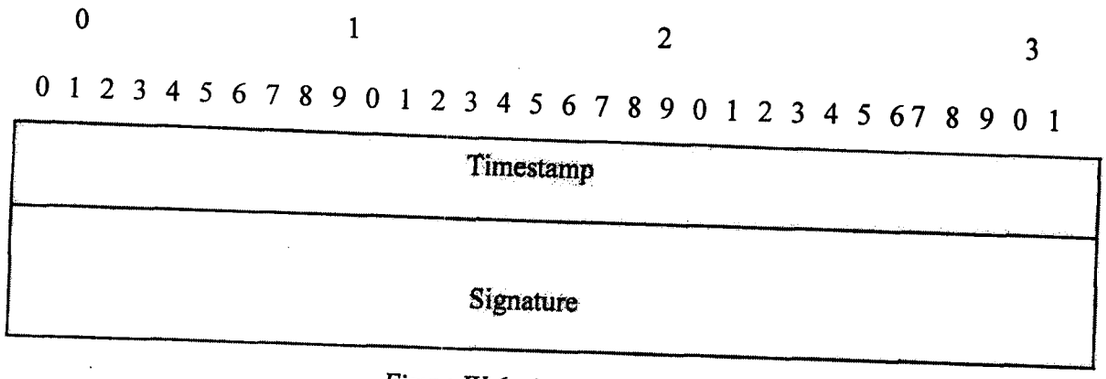


Figure IV-6: signature message format

IV.9.5.Détection d'intrusion dans le réseau AD HOC

Pour contrer les attaques sur les mécanismes de routage de type black hole, ou un nœud malicieux prétend être un relais pour un autre nœud mais ne transmet pas les messages de données, Marti et al. Ont développé deux méthodes appelées watchdog et pathrater. Le watchdog permet d'identifier les nœuds malicieux.

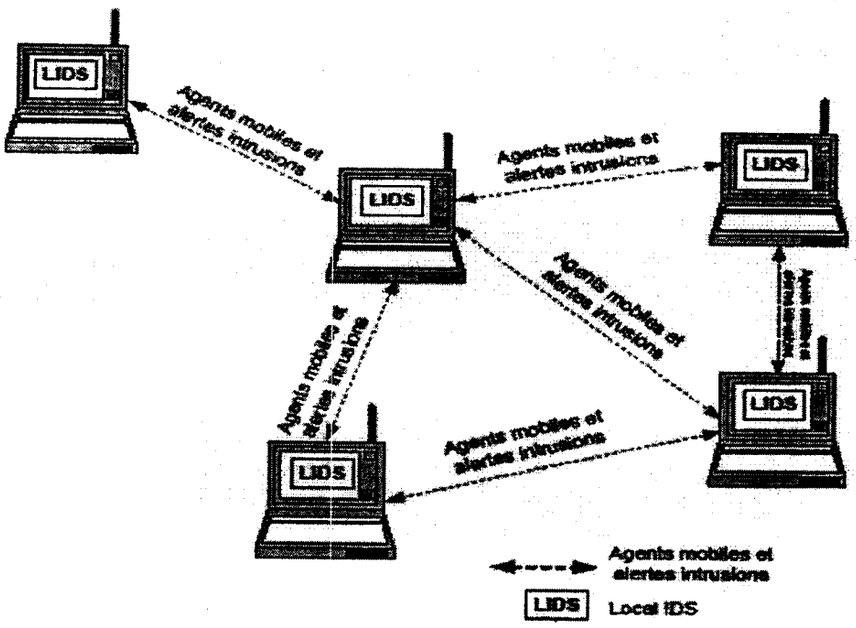
Le pathrater est une technique permettant au protocole de routage d'éviter les nœuds corrompus inscrits dans une liste noire, blacklist. Il faut rester prudent quant à l'utilisation de ces mécanismes car ils peuvent être détournés par un attaquant. En effet, un nœud malicieux peut aussi faire en sorte qu'un nœud valide soit ajouté à la liste noire, l'isolant ainsi du réseau. L'utilisation de détecteurs d'intrusion dans les réseaux ad hoc est une solution complémentaire faisant l'objet de recherches intensives. L'IDS (Intrusion Détection System) collecte et analyse les données du trafic afin de déterminer si des utilisateurs non autorisés sont connectés ou si certains nœuds ont des comportements anormaux.

Un axe de recherche consiste à étudier la manière dont les protocoles de routage pourraient utiliser ces informations pour prévenir certaines attaques.

Une intrusion est toute action visant à compromettre l'intégrité, la confidentialité ou la disponibilité d'une ressource. L'observation des attaques dirigées vers les systèmes d'information nous montre que, quelles que soient les techniques de prévention mises en place contre les intrusions, il existe toujours des failles exploitables pour celui qui les traque. L'attaque d'un système peut même être réalisée simplement à partir de l'enchaînement d'opérations élémentairement autorisées ; elle ne nécessite donc pas toujours de contourner les mécanismes de sécurité. La détection d'intrusions peut donc être considérée comme une action complémentaire à la mise en place des mécanismes de sécurité. En effet, si une tentative d'intrusion est détectée suffisamment tôt, les réponses du système peuvent permettre de limiter les conséquences d'une attaque.

➢ ***Exemple d'architecture IDS distribué pour réseau sans fil ad hoc***

Une solution IDS a été proposée consistant à équiper chaque nœud du réseau d'un système de détection local (LIDS, Local Intrusion Détection System). Les ressources réseaux ne sont utilisées que pour informer les autres nœuds d'une attaque détectée localement et, si nécessaire, pour collecter des informations complémentaires disponibles uniquement sur d'autres nœuds du réseau. L'architecture globale est représentée figure IV-7 [20].



FigureIV-7: architecture globale de l'IDS

Ce modèle d'architecture est basé sur une plate-forme pour agents mobiles. Un agent mobile est défini comme une entité logicielle qui fonctionne de manière autonome et continue dans un environnement particulier, capable de se déplacer et de s'adapter aux changements de l'environnement, de communiquer et de coopérer avec d'autres agents.

Dans ce modèle, les entités logicielles hébergées sur chaque nœud (LIDS) fonctionnent de manière indépendante et observent les activités locales. Le LIDS détecte les intrusions à partir de cette surveillance locale et peut amorcer des réponses en conséquence. Si une anomalie est détectée ou si les signes d'intrusion nécessitent d'être confirmés, des agents mobiles peuvent être créés et envoyés vers d'autres nœuds pour y effectuer des tâches spécifiques et ensuite retourner les informations recherchées.

La mise en œuvre des agents mobiles, qui permet de déplacer le code vers les données à analyser, est une alternative aux architectures clients/serveurs. Cette solution de communication entre les nœuds est efficace si le code de l'agent est moins volumineux que celui des données à analyser [20].

IV.10.Conclusions

Les aspects de confiance du routage ad hoc OLSR ont pu être formalisés grâce au langage choisi, ce qui a permis d'interpréter des attaques contre OLSR en termes de classes et de relations de confiance. Ils en résultent des propositions pour utiliser le raisonnement sur la confiance comme un moyen pour pallier certaines vulnérabilités du protocole.

En effet, l'analyse réalisée fait ressortir des possibles mesures pour rendre OLSR plus fiable et cela en exploitant des opérations et informations déjà existantes dans le protocole, sans recours à des mécanismes cryptographiques.

Nous arrivons à la conclusion que des mécanismes de méfiance envers les comportements Suspects peuvent être mis en place utilisant la corrélation entre les informations fournies dans les messages reçus. Par exemple, la découverte de voisinage, qui est limitée aux informations fournies par le message HELLO, peut être renforcée en exploitant les informations topologiques (messages TC) pour valider les connaissances acquises et déduire d'autres critères qu'un nœud peut avoir pour sélectionner ses MPR.

Des relations entre les nœuds peuvent être dérivées exclusivement par un raisonnement sur la confiance. Ces relations dérivées pourraient être utilisées dans la sélection des MPR. Il est aussi possible d'envisager l'utilisation de la confiance comme un critère additionnel au degré des nœuds (nombre de voisins déclarés) pour calculer la table de routage.

Il est enfin possible à un nœud de découvrir les informations sur la confiance que d'autres nœuds mettent en lui. En principe, tout nœud pourrait considérer la possibilité d'avoir un comportement de réciprocité envers ces nœuds.

Conclusion générale

Dans notre mémoire, nous avons étudié globalement les problèmes de sécurité inhérents aux réseaux mobile ad hoc MANETS, plus précisément les problèmes relatifs aux protocoles de routage. Nous avons donné une analyse des solutions proposées pour sécuriser OLSR dans laquelle nous avons énuméré les différentes attaques et risques liés à la sécurité de ce protocole.

La littérature, qui s'étoffe très rapidement dans ce domaine, offre des solutions pour le problème d'authentification des nœuds, dont les plupart sont basée sur la cryptographie à seuil et le partage de secret, mais ces solutions sont généralement difficiles à implémenter. Des algorithmes d'échange de clefs qui s'adaptent aux caractéristiques des réseaux Ad Hoc sont aussi proposés.

Comme, le routage présente la fonction essentielle dans un réseau, en particulier les réseaux Ad Hoc, la sécurité des protocoles de routage a été pleinement étudié et plusieurs solutions ont été proposées. Ces solutions incluent en première instance l'ajout d'une signature numérique au trafic de contrôle qui est la protection canonique contre les intrusions ainsi que la modification du paquet OLSR par l'insertion d'un champ d'horodatage pour contrecarrer les attaques de replay. Les réseaux ad hoc sont le type le plus utile et souple de réseau sans fil; pour cette raison ils sont largement utilisés dans les environnements militaires. Dans ce contexte, l'information sur la topologie à beaucoup de valeur, et le réseau doit être protégé contre des intrusions qui auraient de lourdes conséquences. En plus des techniques de prévention déjà citées, nous avons aussi décrit brièvement une méthode pour la détection et l'élimination des comportements suspects appelés la méthode de détection d'intrusion (IDS).

Cette méthode vise à déceler les nœuds qui ne respectent pas le protocole et perturbent le bon fonctionnement du réseau. Une fois que les nœuds malveillants on été identifiés, une alerte est envoyée pour informer le reste du réseau. Les autres nœuds mènent ensuite une action conjointe pour éliminer les nœuds malveillants du réseau, par exemple en les effaçant des tables de routage. Ce système de détection peut être utilisé en synergie avec les techniques de prévention.

Ce mémoire nous a permit de collecter plusieurs informations concernant le réseau ad hoc et les protocoles de routage les plus adapté pour ce type de réseaux ; Sans oublier qu'on a très bien saisit le fonctionnement du protocole OLSR, les challenges qui le confronte et les solutions proposées pour le sécurisé et garantir une fiabilité et sûreté des communications entre nœuds mobiles.

References bibliographies

[1] S. Carson and j. Macker, « RFC 2501: Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations » January 1999.

[2] I. Khemapech, L Duncan and A. Miller, « A Survey of Wireless Sensor Networks Technology» School of Computer Science University of St Andrews, 2005.

[3] C. chaudet, « Autour de la réservation de bande passante dans tes réseaux Ad hoc » Thèse de doctorat, INSA Lyon, Septembre 2004.

[4] P. Tortelier «les réseaux Ad hoc »FTR&D/DMR, 2002.

[5] I. armulles, T. Robles, I. Ganchev, M. O'droma » H. Chaouchi and M. Siebert « On Ad hoc Networks in me 4G Integration Process » ANWIRE Project TF1.5, wwwjmwire.org.

[6] M. Coupechoux, « Protocoles distribués de contrôle d'accès au médium pour réseaux Ad hoc fortement chargés » Thèse de doctorat, ENST, Paris, Juin 2004.

[7] IEEE, Groupe de travail 802.11 : « http y/grouper.feee.org/groups/802/11/ ».

[8] H. Moustafa « Routage unicast et multicast dans les réseaux mobiles Ad hoc » Thèse de doctorat, ENST, Paris, Décembre 2004

[9] D. Simplot-Ryl « Réseaux sans fils de nouvelles génération », Université Lille 1,2004.

[10] CERT http://www.cert.org/tech_tips/denial_of_service.html.

[11] R. Benzair, « Réseau mobile Ad-hoc : protocoles de routage, simulation du protocole OLSR» Rapport de DEA, Université de Versailles-Saint Quentin, 2001.

[12] F. Risson et N. Gaona, « Le routage au sein des Réseaux Ad hoc » Master Informatique
Systèmes Informatiques & Réseaux, Projet Bibliographique, Décembre 2004.

[13] I. Jawhar and J. Wu, « Quality of Service Routing in Mobile Ad hoc Networks» Florida Atlantic University, Boca Raton, Kluwer Académie Publishers, 2004.

[14] C.E. Perkins, E.M. Royer, S.R. Das, « Quality of service for Ad hoc on-demand distance C.E. vector routing » , IETF Internet Draft, draft-ietf-manet-aodvqos- OO.txt, July 2000.

[15] M. Guerrero Zapata, « Secure Ad hoc On-Demand Distance Vector (SAODV) Routing» draft-guerrero-manet-saodv-OO.txt, Nokia Research, August 2001.

[16] T. Causen ET P. Jacquet "optimized link state routing protocol (OLSR).

[17] http://hipercom.inria.fr.

[18] C.Omar, « sécurité des réseaux Mesh ».

[19] D.raffo « Security Schemes for the OLSR Protocol for Ad Hoc Networks».

[20] B.Jouga, « Détection d'intrusion dans les réseaux AD HOC».

Acronymes & *Abréviations*

4G	4th Generation
API	API (Application Programming Interface)
ANSN	Advertised Neighbor sequence Number
AODV	Ad Hoc Ondemand Distance Number
AP	Access Point
BLR	Boucle Locale Radice
BSS	Basic Service Set
CBRP	Cluster Based Routin Protocole
CEPT	Conférence Européenne des postes de Télécommunication
CPU	Central processing Unity
CGSR	Cluster head Geteway Switch Routing
DREAM	Distance Routing Effect Algorithm for Mobility
DSDV	Dynamic destination Sequenced Distance Vector
DSR	Dynamic Source Routing
EDGE	Enhanced Data rato for Global Evaluation
ESS	Extented Set Service
ESSID	Extented Set Service Identifier
ETSI	Europeen Telecommunication Standards Institute
FCC	Federal Communication Commission
FH	Frequency Hopping
FSR	Fish-eye State Routing
GGAR	Geocast Geographic Addressing and Routing
GPRS	General Paket Radio Service
GPSR	Greedy Perimeter Stateless Routing
GSM	Global System for Mobil
GSR	Global State Routing
GPS	Global Positionnement System
HSDPA	High Speed Downlink Packet Access
HSR	Hierarchical State Routing
IBSS	Independent Basic Service Set
IDS	Intrusion Detection System
IntServ / RSVP	Integrated Services/ Reservation Protocol
IEEE	Institute Of Electrical and Electronic Engineers
IR	Infra red.
ISM	Industrial Scientific and Medical.
LAR	Location-Aided Routing.
LIDS	Local Intrusion Detection System.
LSP	Link State Packet.
MANET	Mobile Ad hoc NETwork.
MIB	Management Information Base.
MPR	Multi Point Relays.
MRL	Message Retransmission List.
MSN	Message Sequence Number.
NS	Numéro de Séquence.

Acronymes & *Abréviations*

OFDM	Orthogonal Frequency Division Multiplexing.
OLSR	Optimized Link State Routing.
PEA	Patch-Finding Algorithm.
PSN	Packet Sequence Number
PAMAS	Power-aware Multi-access Protocol with Signalling.
RDMAR	Relative Distance Micro-discovery Ad hoc Routing.
RADAR	Radio Detection and Ranging
SSR	Signal Stability-Based Routing.
TC	Topology Control.
TM	Terminal Mobile.
TORA	Tomporary Ordening Routing Algorithm.
TTL	Time to Live.
UMTS	Universal Mobile Telecommunication System.
WLL	Wireless Local Loop.
WLAN	Wireless Local Area Networks.
WMAN	Wireless Metropolitan Area Networks.
WPAN	Wireless Personal Area Network.
WRP	Wireless Routing Protocol.
WWAN	Wireless Wide Area Networks.
ZHLS	Zone Based Hierarchical Link State Routing
ZRP	Zone Routing Protocol.