REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEINEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MENTOURI CONSTANTINE
FACULTE DES SCIENCES DE L'INGENIEUR
DEPARTEMENT D'ELECTRONIQUE

Ecole Doctorale des Technologies et des Applications Spatiales
Laboratoire d'Electromagnétisme et Télécommunications

MEMOIRE

Présenté pour obtenir le diplôme de Magister
(Option : Télécommunications Spatiales)

Thème :

Architecture et politique de robustesse par Multihoming dans les réseaux ad hoc et les réseaux satellitaires

Présenté Par

TALBI HAMZA

Devant le **JURY**

Président du jury : RIABI Med lahdi Professeur université de Constantine
Rapporteur : CHAABI Abelhafid Professeur université de Constantine
Examinateur : BENSLAMA Malek Professeur université de Constantine
Examinateur : HAMMOUDI Zoheir Professeur université de Constantine

Dédicace

- A mes parents durant mon existence et ma scolarité,
- A Mes frères et Mes sœurs,
- A tous les enseignants de l'école doctorale EDTAS,
- A tous les étudiants de l'école doctorale EDTAS,
- A tous mes amis,
- J'exprime mes sentiments les plus profonds et,
- Leurs dédie ce modeste travail

TALBI HAMZA.

Remerciements

Je tiens à remercier dieu tout puissant de nous avoir donnés courage et force pour réaliser ce travail.

le Professeur M.BENSLAMA professeur du laboratoire de recherche en Electromagnétisme et Télécommunication (LET) à l'université de Constantine, pour m'avoir proposé ce sujet

Je tiens à exprimer mes plus vifs remerciements, avec beaucoup de respect et de confiance, mon encadreur le Professeur Abelhafid Chaabi, professeur à l'université de Constantine, pour son aide, ses conseils, avec un enthousiasme toujours égal.

Je tiens à remercier monsieur le Professeur Med.L.Riabi, d'avoir accepter de présider mon jury.

Je voudrais exprimer aussi mes reconnaissances à Messieurs :

Z. HAMMOUDI Professeur à l'université de Constantine, Ml.BENSLAMA Professeur à l'Université de Constantine qui sont les membres de jury de ce mémoire. Je tiens à les remercier pour l'intérêt qu'ils ont porté à mon travail et leurs remarques judicieuses.

J'adresse mes vifs remerciements les plus chaleureux à l'ensemble des enseignants de l'école doctorale EDTAS qu'ils n'ont pas épargné d'effort pour notre formation et la bonne marche de cette école.

A mes parents, mes frères et soeurs, et mes amis,

J'adresse mes vifs remerciements, pour leurs encouragements et leurs aides. Je tiens à exprimer mes remerciements à mes amis et mes collègues.

MERCI

Abstract:

Ad hoc networks witch operate without the prior existence of any infrastructures, or central administration manage the communication robustness at the network level by their routing protocols proactive vs reactive. In case of route breakages or failure of an interface, the routing protocol is in charge of the route recovery. The goal of this thesis is to improve the robustness by adding redundancy based on multihoming capacity. Thus, in case of failure, traffic will be switched to a backup path. Redundancy methods have been studied at different levels. At the network level and at the transport level by the SCTP protocol that is able to manage multihoming. work in the thesis will focus on the definition of a multihoming architecture. the multipath routing, the SCTP behaviour and the cross layer communication related to the network and transport levels. Moreover, an evaluation study of the robustness improvement regarding the network topology dynamicity will be undertaken, we chose the HIP cross layer as an interface between these two levels

In the following we studied the characteristic of the SCTP protocol over satellite links, we note that the are a number of improvements in throughput and delay of these networks

Résumé :

Les réseaux ad hoc, qui fonctionnent sans l'existence préalable de toute infrastructure ou administration centrale, ces réseaux assurent la robustesse des routes entre une source et une destination par leurs protocoles de routage proactifs vs réactifs, cependant ces protocoles sont de nature unipath c.à.d. un seul chemin existe à la fois entre une source et un destinataire donnée L'objectif de ce mémoire est de définir une architecture d'un réseau ad hoc avec des nœuds multicartes. Ainsi en cas de panne d'un lien ou d'une interface, le trafic est basculé sur un chemin de secours. La gestion de la redondance a été étudiée au niveau du réseau, par des algorithmes de routage multichemins, et au niveau du transport par le protocole SCTP. La première étape de ce mémoire sera de définir une architecture de multihoming multi niveaux, en précisant le protocole de routage multichemins, le fonctionnement du protocole SCTP ainsi qu'aux communications inter couches transport et réseau, nous avons choisi la couche HIP comme une inter couches entre ces deux niveaux

Dans la suite nous avons étudié les caractéristiques du protocole SCTP, sur des liaisons satellitaires, nous avons remarque qu'il y a des améliorations dans le débit et le délai de ces réseaux

ملخص:

شبكات الكمبيوتر المستقلة أومآ يعرف ب ‘‘أد هوك’’ تسمح لأجهزة الكمبيوترالنقالة الإتصال فيما بينها دون أي تثبيت مسبق للهياكل القاعدية.هده الشبكات تمكنت من تثبيت متانة وفعالية الطرق بين المصدرو والمقصد بواسطة بروتوكولات التوجيه. الهدف من هذه المدكرة هو زيادة هذه الفعالية بإضافة تكرار في الطرق بحيث عند حدوث انقطاع في المسار الأولي فإن نقل المعلومات يوجه إلى المسار الاحتياطي.

و قد درست إدارة التكرار في الشبكة على مستوى طبقة الشبكة، بواسطة خوارزميات التوجيه المتعددة، وأيضا في مجال طبقة النقل كما يتضح من بروتوكول SCTP. كما يمكن تنفيذها على ربط البيانات المتعددة المعدات. المرحلة الأولى من هذه المدكرة هو تجميع هذا العمل لتحديد بنية على مستوى طبقة النقل بواسطة معدات أجهزةإعلام ألي متعددة الأوجه، وكما يحدد نظام الإصدار IPv6 لمعالجة عناوين الشبكات IPv6 متعددة الاوجه ، وبروتوكول التوجيه متعددة المسار، وتشغيل بروتوكول SCTP فضلا عن اتصال بين طبقات الشبكة و النقل. وعلاوة على ذلك ستعمل القوة النسبية الناجمة عن وظيفة multihoming من التحكم في ديناميكية و طبولوجيا شبكات ‘‘أد هوك’’ .

وقمنا أيضا بدراسة خاصيتي بروتوكول النقل SCTP ultistreamingM و Multihoming عندما يتعلق بشبكات الأقمار الصناعية (rrédiumi) والخلاصة هي مجموعة من الاقتراحات لتعديل قيمة وسائط البروتوكول لتتماشى مع هذا النوع من الشبكات

SOMMAIRE

Chapitre 1 : généralité sur les réseaux ad hoc

Chapitre 2 : le routage Multi-chemins dans les réseaux ad hoc

Chapitre 3 : auto configuration d'adresses IP pour les réseaux ad hoc

Chapitre 4 : Le niveau transport pour les réseaux ad hoc

Chapitre 5 : Optimisation par cross layer

Chapitre 6: le protocole SCTP dans les réseaux satellitaire

Liste des sigles et Abréviations :

ACN	Address Conflict Notice
ATCP	Ad hoc TCP
AODV	Ad-Hoc On-demand Distance Vector
AOMDV	Ad-Hoc On-demand Multipath Distance Vector
AWND	Advertised Window
BER	Bit Error Rate
BSS	Basic Set Service
CDMA	Code Division Multiple Access
CLI	Cross layer Interface
CSMA /CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear To Send
CWND	Congestion Window
DAD	Duplicate Address Detection
DAMA	Demand Assignment Multiple Access
DAP	Duplicate Address Probe
DCF	Distributed Coordination Function
DHCP	Dynamic Host Control Protocol
DIFS	DCF Inter-Frame Spacing
DNS	Domain Name System
DSDV	Destination Sequenced Distance Vector
DSL	Data Subscriber Line
DSR	Dynamic Source Routing
DVB	Digital Video Broadcasting
DVB-RSC	Digital Video Broadcasting-ReturnChannel
ECN	Explicit Congestion Notification
ESS	Extented Service Set
FDMA	Frequency division Multiple Access
FTP	File Transfer Protocol
GEO	Geostationary Earth Orbit
HIP	Host Identity Protocol
HIT	Host Identity Tag
HOL	Head Of Line
IBSS	Independent BSS
IDD	Inter-packet Delay Difference
IETF	Internet Engineering Task Force
IP	Internet Protocol
IRIS	Internet Routing in Space
ISL	Inter-Satellite Links
ISP	Internet Service Provider
ISO	International Standardization Organization
LLC	Logical Link Control
LEO	Low Earth Orbit
MAC	Medium Access Control
MAN	Mobile Metropolitan ad hoc Network
MANET	Mobile Ad-hoc NETwork
MEO	Middle Earth Orbit
MPR	Multi-Points Relay

MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NAV	Network Allocation Vector
NCC	Network Control Centre
NIS	Number Inbound Stream
NOS	Number of Outbound Stream
NS	Network Simulator
OFDM	Orthogonal Frequency Division Multiplexing
OLSR	Optimized Link State Routing
OOO	Out Of Order
OSI	Open System Interconnection
PACMAN	Passive Auto Configuration for Ad hoc Mobile Network
PCF	Point Coordination Function
PLR	Packet Loss Ratio
POR	Packet Out of Order
RFC	Request For Comment
RIP	Routing Internet Protocol
RMPSR	Robust MultiPath Source Routing
RREQ	Route Request
RREP	Route Response
RSR	Redundant Source Routing
RTC	Request to Call
RTC	Request to Send
RTO	Retransmission Time Out
RTS	Request To Send
RTT	Round Trip Time
RWP	Random WayPoint
SCTP	Stream Control Transmission Protocol
SDMA	Space Division Multiple Access
SIFS	Short Inter-Frame Spacing
SMR	Split Multipath Routing
SNR	Signal to Noise Ratio
TCP	Transmission Control Protocol
TCP-BuS	TCP Buffering capability and Sequence information
TCP-DOOR	TCP Detection of Out-Of-Order and Response
TDMA	Time Division Multiple Access
TPSN	TCP Packet Sequence Number
TWND	Transmission Window
UDP	User Datagram Protocol
VSAT	Very Small Aperture Terminal
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Wide Area Network
WPAN	Wireless Personal Area Network
ZRP	Zone Routing Protocol

Table des figures :

Introduction générale :

Un réseau ad hoc est un ensemble d'entités mobiles interconnectées par une technologie sans fil formant un réseau temporaire sans l'aide de toute infrastructure ou d'une administration centrale, les nœuds eux même forment une infrastructure d'une manière ad hoc, cependant la mobilité des nœuds, résulte une topologie dynamique et une rupture fréquente des liens existe entre les différents nœuds. Les protocoles de routage standardisés par l'IETF "Internet Engineering Task Force" sont des protocoles de type mono-chemin c'est-à-dire, une seule route à la fois existe entre une source et un destinateur donné; La rupture de cette route demande un nouveau processus de découverte de la route afin de trouver un autre chemin valide vers le destinataire.

Les protocoles de routage à chemins multiples peuvent résoudre ce problème par la découverte de plusieurs chemins, l'un est défini comme un chemin primaire et les autres sont des chemins alternatifs. En cas d'une panne dans le chemin primaire, le transfert des données sera commuté d'une manière systématique vers un chemin alternatif. Cette solution augmente les performances d'un réseau ad hoc par la diminution du temps de transfert des données et d'une forte tolérance aux différentes ruptures de la route

Le multidomiciliés ou le "multihoming" (c'est l'accessibilité d'un nœud via plusieurs interfaces réseau) est une autre solution pour créer une redondance des routes entre deux nœuds, où chaque interface peut créer un chemin distinct. S'il y a une rupture de chemin vers une interface, le trafic est basculé vers une autre, cette solution augmente aussi la fiabilité et la robustesse des routes dans un réseau ad hoc, cependant au niveau transport le protocole TCP ne gère pas ce type de connexion. SCTP est un protocole proche de TCP, conçu spécialement pour gérer ce type de connexion a le pouvoir de gérer des équipements dotés de plusieurs interfaces réseau, mais le problème posé qui est le cœur de notre étude, c'est lorsqu'il y a une rupture dans la route, au lieu que le nœud source continue le transfert d'une manière systématique, il génère une requête pour chaque interface, "le problème des requêtes superflues". Dans ce travail nous avons cherché à optimiser le protocole SCTP par l'utilisation d'une communication inter-couches.

L'optimisation par une cross layer n'est pas une idée nouvelle, cela est due à la problématique dans l'architecture actuel TCP/IP, avec la mauvaise interaction entre les différentes couches notamment lorsque il s'agit d'un réseau mobile, ainsi que de nombreuses proposions sur les réseaux sans fil sont basés sur cette approche.

Le mémoire est organisé en cinq chapitres :

Le chapitre 1 est organisé comme suit, après une présentation d'une architecture globale d'un réseau, nous avons fait une étude approfondis sur les réseaux ad hoc, nous avons déterminé leurs caractéristiques et leurs applications. Nous présentons un ensemble de protocoles de routage chacun appartenant à une catégorie distincte, nous terminons ce chapitre avec une simulation montrant les faiblesses et les puissants de chaque protocole.

Le chapitre 2 est focalisé sur un type de routage qui est le routage multichemin, nous commençons ce chapitre par une comparaison entre deux protocoles de routage DSR et AODV dans le cas d'une rupture de la route, puis nous allons présenter quelques protocoles

de routage multichemin .nous terminons ce chapitre par une comparaison entre le protocole AODV et sa version multichemin AOMDV.

Dans le chapitre 3, nous présentons le problème d'auto configuration des nœuds d'un réseau ad hoc, c'est-à-dire comment un nœud acquis une adresse IP, ainsi que les différents mécanismes qui garantissent l'unicité de cette adresse durant la période d'existence d'un nœud dans le réseau ad hoc.

Après avoir fait un exposé global sur le protocole TCP, nous nous sommes penchés sur le problème du protocole TCP dans les réseaux ad hoc et les différents solutions puis nous faisons une étude exhaustive sur le protocole de transport SCTP, ce nouveau protocole de transport hérite des mêmes caractéristiques du TCP, ainsi il ajoute de nouveaux concepts qui peuvent augmenter les performances d'un réseau soit en terme de sécurité par le mécanisme des cookies ou par le concept de multistreaming.

Dans le chapitre 5, nous présentons notre solution qui est basée sur la notion "cross layer". Elle consiste à insérer une sous-couche entre la couche transport et la couche réseau. Le principe de cette inter-couche est inspiré de la spécification HIP "Host Identifier Protocol", son objective est de limiter le rôle d'une adresse IP en un simple routage et pour son rôle d'identification, nous avons créés un nouveau identificateur. L'adresse IP reste seulement un élément de routage. Cette approche peut résoudre certains problèmes dans les réseaux IP tel que le problème de la mobilité et le problème de multihoming.

Dans le chapitre 6, nous présentons, une étude sur le protocole SCTP pour des réseaux satellitaires et des simulations sur ce protocole. Nous concluons ce chapitre avec un ensemble de recommandations sur le protocole SCTP, lorsqu'il est implémenté sur des réseaux satellitaires

Chapitre 1 :

Les réseaux ad hoc

1. Introduction

Les réseaux ont pour fonction de transporter des données d'une machine terminale à une autre, en effet une série d'équipements matériels et de processus logiciels sont mis en œuvre pour assurer ce transport, depuis les câbles terrestres ou les ondes radio dans lesquels circulent les données jusqu'aux protocoles et règles permettant de les traiter.

Du fait du grand nombre de fonctionnalités implémentées dans les réseaux, l'architecture de ces derniers est particulièrement complexe. Pour tenter de réduire cette complexité, les architectes réseau ont décomposé les processus à l'œuvre dans les réseaux en couches protocolaires ou niveaux. Un tel découpage permet au réseau de traiter en parallèle les fonctions attribuées aux différentes couches.

Chaque niveau N, est identifie par trois objets [1] qui sont :

- le *Protocole N* : qui est description formel de règles et de conventions à suivre dans un échange d'informations, que ce soit pour acheminer les données ou pour que le destinataire comprenne comment il doit utiliser les données qu'il a reçues,
- le *Service N* : qui désigne le service qui doit être rendu par la couche N à la couche supérieure (N + 1). Ce service correspond à un ensemble d'actions incluant d'événements et des primitives,
- les *Points d'accès* **:** sont les frontières entre deux couches adjacentes à travers lequel un service passe d'une couche à l'autre

2. La normalisation des réseaux :

Historiquement chaque constructeur informatique définit sa propre architecture réseau, (SNA pour IBM, BULL pour NEC,…) L'Incompatibilité et la non-interopérabilité entre ces systèmes [2] montrent l'impuissance de ces architectures. Des travaux aboutis à des architectures unifiées et qui permettent l'interconnexion d'équipements de différents constructeurs, les deux grandes architectures qui se disputent actuellement le marché mondial des réseaux sont :

2.1 l'architecture **OSI** (Open Systems Interconnection)**:**

"L'International Standardization Organization" (ISO) a défini un modèle de référence appelé modèle OSI porte le sigle "ISO IS7498", ce modèle définit sept niveaux différents pour le transfert de données entre les systèmes. Ces niveaux sont également appelés couches

1. **Couche physique :** cette couche s'occupe de normaliser les caractéristiques électriques, mécaniques, et les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données.
2. **Couche liaison de données :** La fonction principale de cette couche c'est la délimitation des paquets, lors de l'arrivée des éléments binaires le récepteur ayant le pouvoir de connaître le début et la fin de la trame, d'autres fonctions comme la correction d'erreurs, la synchronisation … etc. sont assurés par cette couche.
3. **Couche réseau :** C'est la couche qui permet d'acheminer les données vers le récepteur donné on choisissant le bon chemin, l'autre fonction est l'interconnexion des différents réseaux entre eux.

4. **Couche de transport :** est chargée de la segmentation des données applications en paquets (datagrammes) adaptés pour la transmission jusqu'au destinataire sur les infrastructures réseau, ainsi elle procure des mécanismes permettant le contrôles de la quantité des données injectées dans le réseau.
5. **Couche session** : Cette couche organise et synchronise les échanges entre tâches distantes. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue.
6. **Couche de présentation :** cette couche assure l'unicité de langage c'est-à-dire que l'information envoyée par la couche application d'un système est lisible par la couche application d'un autre système.
7. **La couche application :** Cette couche est le point de contact entre l'utilisateur et le réseau. donc elle offre à l'utilisateur les différents services apporter par le réseau, comme par exemple le transfert de fichier, la messagerie...etc

2. 2 L'architecture Internet :

L'autre architecture dite TCP/IP, qui est la source du réseau Internet actuel, Elle est adoptée par de nombreux réseaux privés, tel que les intranets. TCP/IP aussi définit une architecture en couches qui inclut également, sans qu'elle soit définit explicitement, une interface d'accès au réseau, ces couches sont :

1. **couche application** : Le modèle TCP /IP regroupe en une seul couche tous les protocoles de haut niveau relatif au contrôle de dialogue
2. **couche transport :** sa fonction résume dans l**'**établissement et la fermeture des connexion, résoudre tous les problèmes liées au transmission des paquets dans les niveaux inférieurs tel la perte, la duplication et d'erreur
3. **couche Internet :** cette couche assure principalement la fonction d'adressages et de routage entre les différents sous-réseaux.
4. **couche accès au réseau :** le modèle TCP/IP ne spécifie pas les détails de cette couche, ce qui permet a plusieurs type de réseaux de s'intégrer dans l'architecture globale TCP/IP.

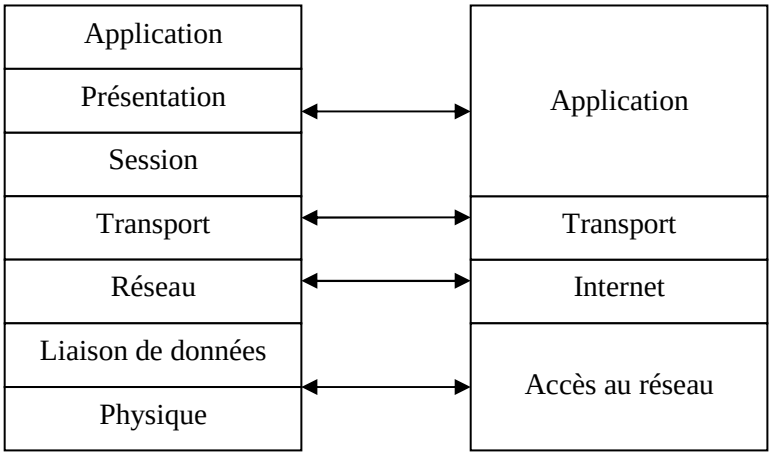


Figure 1.1 : Modèle de référence OSI et TCP/IP

3 Les réseaux sans fil IEEE 802.11 :

Les réseaux sans fil sont en plein essor, ce type de réseaux permettent à l'utilisateur de changer de place tout en restant connecté au réseau, la flexibilité, la souplesse d'utilisation, le coût faible, le déploiement facile et rapide (absence du câblage), sont les avantages de ce type de technologie, plusieurs gammes sont actuellement commercialisées, leurs différence résident dans la taille de la zone à couvrir, Les principales normes pour ce types de réseaux sont [1] :

- IEEE 802.15 : pour les petits réseaux ou PAN "Personnel Area Networks" exemple le "Bluetooth".
- IEEE 802.11 : pour les réseaux locaux WLAN "Wireless Area Networks".
- IEEE 802.16 pour les réseaux métropolitain ou WMAN "Wireless Metropolitain Area Networks"connu sous le nom commercial WIMAX.
- IEEE 802.20, IEEE 802.22 : pour les réseaux régionaux, WRAN "Wireless Regional Area Networks" dont le rayon de la cellule peut atteindre un diamètre de 30 Km, et permet le transport des données multimédia.

Le 8021.11 est un standard de l'IEEE pour les réseaux locaux sans fil, la première version du standard date de l'année 1997, comme toutes les normes définies par le comité 802, IEEE 802.11 couvre les deux premières couches du modèle OSI [6], la couche physique et la couche liaison de données figure 1.2, le standard initial définit trois couche physique différentes [6], [7] pour les réseaux 802.11 :

- IR (Infrarouge)
- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)

L'infrarouge n'est utilisé que dans les cas où les distances entre les différentes stations sont faibles. Le FHSS et le DSSS utilisent la bande des 2,4 GHz de l'ISM (Industrial, Scientific, and Medical) l'une comme l'autre permettant d'atteindre des débits allant jusqu'à 2 Mbit/s. Ultérieurement d'autres extensions du standard sont apparus (802.11*a*, 802.11*b*, .c, .d,…, .m) et qui apportent une augmentation considérable dans le débit de transmission, allant de 11 Mb/s pour le 802.11.b à 54 Mb/s pour le 802.11.a, leurs principales différence résident dans le type de modulation utilisé OFDM (Orthogonal Frequency Division Multiplexing) ou de type CDMA, d'autres standard introduisent des mécanismes supplémentaires pour améliorer la sécurité notamment ce type de réseaux est plus vulnérable [5]. La version 802.11.n une révolution dans les réseaux WLAN et offrant un débit théorique allant jusqu 540 Mb/s, grâce une technologie MIMO "Multi-IN Multi-Out" et une modulation OFDM.

<table>
<tr><td rowspan="2">Couche Liaison des données</td><td colspan="7">802.11 LLC (Logical Link Control)</td></tr>
<tr><td colspan="7">802.11 MAC (Medium Access Control)</td></tr>
<tr><td>Couche physique</td><td>802.11 infrarouges</td><td>802.11 FHSS</td><td>802.11 DSSS</td><td>802.11.a OFDM</td><td>802.11.b HR-DSSS</td><td>……..</td><td>802.11.n MIMO-OFDM</td></tr>
</table>

Figure 1.2 : couche 1 et 2 du standard 802.11

La couche liaison de données du protocole 802.11 est composée essentiellement de deux sous-couches, LLC “Logical Link Control” et MAC “Medium Access Control” cette sous-couche détermine la manière d’accès au canal. Tandis la couche LLC cache les détails de la couche elle utilise les mêmes propriétés que la couche LLC IEEE 802, de ce fait il est possible de relier un WLAN à tout autre réseau local appartenant à un standard de l’IEEE [3].

3.1 Architecture d’un réseau sans fil IEEE 802.11 :

Le standard IEEE 802.11 permet l’interconnexion des terminaux sans l’utilisation de câble, cependant deux modes sont standardisés pour permettre un dialogue entre les stations distantes [7], le premier est le mode infrastructure qui requiert la présence d’un AP “ Access Point” pour fournir aux différent station des service spécifique, sur une zone de couverture déterminé nommée BSS “Basic Set Service ” similairement au réseau cellulaire, un réseaux sans fil peut composer de plusieurs BSS connectées entre eux par un câble ou par voie hertzien figure 1.3 , Un terminal peut déplacer d’un BSS à un autre s’appel sans rupture de connexion “roaming“ [1], la gestion du transfert des données ou la mobilité des terminaux entres les différents BSS se fait sous la direction d’un système de distribution ou ESS “Extended Set Service”.

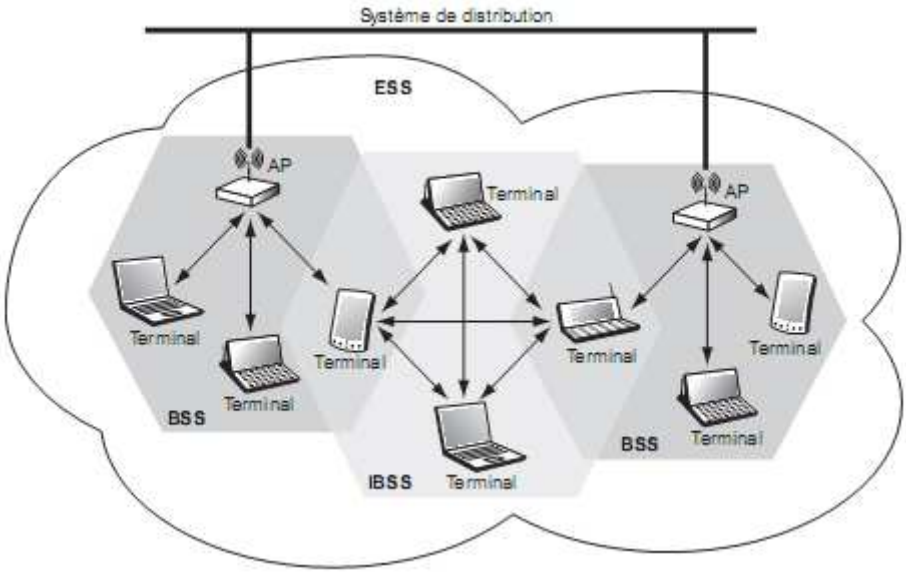


Figure 1.3 Architecture d’un réseau sans fil 802.11

L’autre mode standardisé est le mode Ad-hoc, ou IBSS “Independent BSS” qui ne nécessite aucune infrastructure, ou un système de distribution central. Chaque station peut établir une communication avec n’importe quelle autre station dans le réseau sans obliger de passer par un point d’accès.

3.2 La méthode d’accès CSMA/CA :

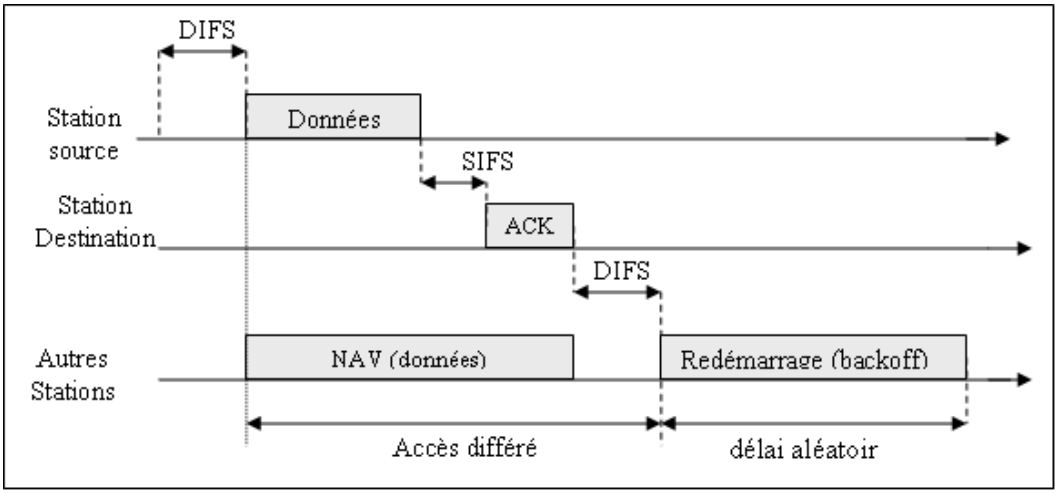
Comme la détection des collisions n’est pas possible dans un réseau hertzien [1], la norme IEEE 802.11 utilise la CSMA/CA “ Carrier Sense Multiple Access with Collision Avoidance” comme technique d’accès au canal, cette technique basé sur l’évitement des collisions par l’utilisation des ***temporisateurs*** *DIFS* “DFC Inter-Frame Space et *SIFS* “Short Inter-Frame Space” [10], [7] et des ***trames d’acquittement ACK.***

La méthode CSMA/CA un peut similaire à la technique utilisée par les réseau IEEE 802.3, avec une particularité, les deux utilisent “écoute avant de parler” c’est-à-dire avant d’émettre les stations écoute le médium, leur différence réside dans la manière de traitement des

collisions, quand la détection est impossible dans les réseaux sans fil, le standard utilise une technique qui permet d'éviter les collisions

IEEE 802.11 propose aussi deux modes d'accès au canal radio, un mode centralisé (PCF pour Point Coordination Function) qui nécessite l'utilisation d'un *AP* pour gérer les accès et un mode distribué DCF pour "Distributed Coordination Function" qui défini une méthode d'accès par contention, où chaque terminal prend seul la décision d'accéder au canal ou de retarder sa transmission. Ces deux modes d'accès au médium peuvent être utilisés dans le mode infrastructure alors que seul le DCF est possible dans le mode ad hoc [7]

La figure ci-dessous illustre le processus de transmission des trames à partir d'un émetteur.



ACK (ACKnowledgement): acquittement DCF (Distributed Coordination Function)
DIFS (DCF Inter-Frame Spacing) NAV (Network Allocation Vector)
SIFS (Short Inter-Frame Spacing)

Figure 1.4 : Processus de transmission des trames dans le standard 802.11

On décrit ici brièvement le processus d'échange des données dans un réseau IEEE 802.11 .une station qui veut établi une communication, elle commence par une écoute du médium, si au bout d'un intervalle de temps DIFS le médium est libre la station source commence son transfert des données. Si les données envoyées sont reçues intactes, la station destination attend pendant un temps équivalent à un SIFS et émet un ACK pour confirmer leur bonne réception, Le non-retour d'un accusé de réception au bout d'un intervalle de temps prédéterminé, permet de détecter qu'il y eu une collision. On note que la valeur du timer SIFS est plus petit qu'un DIFS cela permet d'empêcher qu'une autre station de le considéré comme DIFS.

Quand il y a un transfert des données, les autres stations l'entendent et, pour éviter une collision, mettent à jour un timer, appelé NAV (Network Allocation Vector), permettant de retarder toutes les transmissions prévues. La valeur du NAV est calculée par rapport à l'information située dans le champ durée de vie, ou TTL (Time To Live), contenu dans les trames qui ont été envoyées. Les autres stations n'ont la capacité de transmettre qu'après l'expiration du NAV.

3.3 Problème du nœud caché :

Un problème célèbre spécifique aux environnements sans fil, il est apparu lorsqu'il y un obstacle ou une longue distance entre les nœuds [10],[3], La situation correspondante à ce

problème est illustrée au Figure ci-dessous, ici la station *C* peut communiquer respectivement avec *A* et *B*. mais A ne peut entendre l'activité de B et réciproque, sa est due d'un obstacle ou da la distance une donc une collision peut apparaître au niveau du nœud C , si l'une des station A ou B entrain de transmis ses données vers le nœud C et l'autre ne sais pas considère le medium radio libre hors sa portée

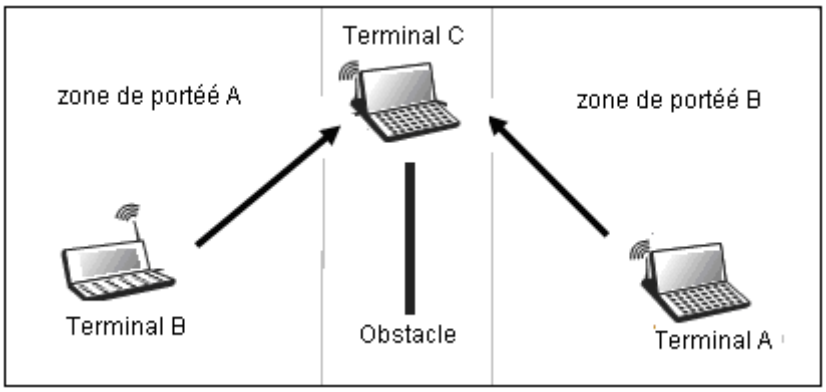


Figure1.5 : Problème du nœud caché

3.3.1 Le mécanisme RTS "Request to Send" CTS "Clear To Send":

Ce problème est résolu par la couche MAC [7], pour empêcher l'apparition d'une telle situation, Le mode DCF fournit un mode optionnel d'échange de paquets de contrôle appelés RTS/CTS. Illustré dans la figure1.6.

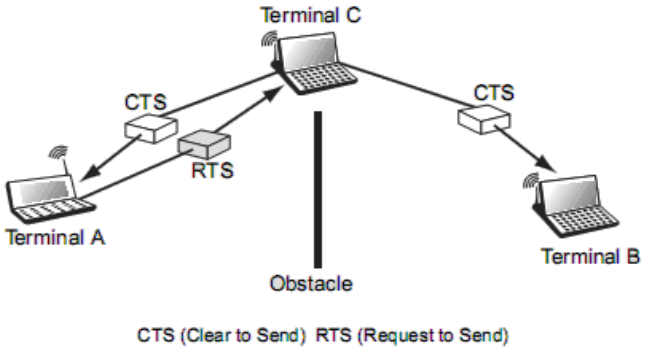
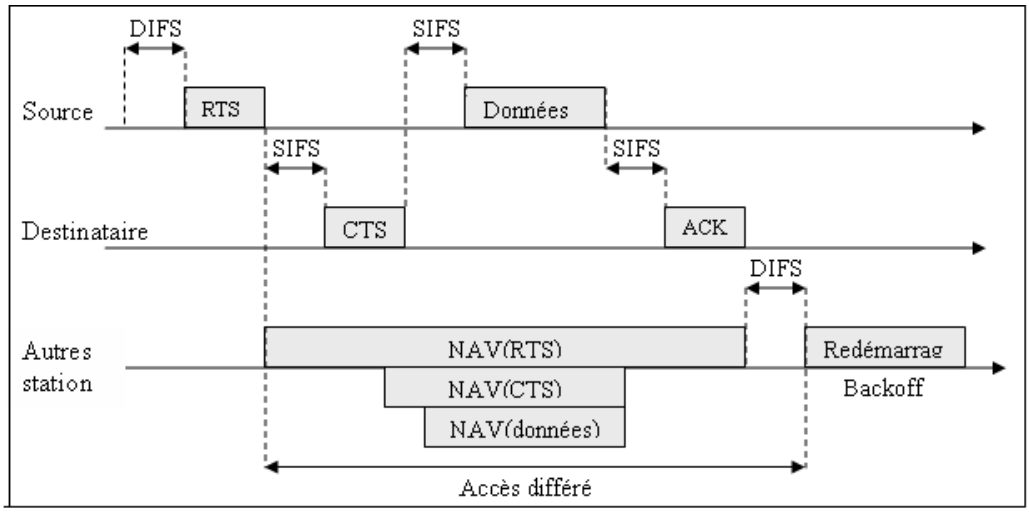


Figure 1.6 mécanisme de résolution du problème de nœud caché

Le scénario suivant décrit le processus de résolution du problème, avant de transmettre ses données, un émetteur envoie un paquet de contrôle RTS (Request to Send) à son destinataire. Tous les mobiles à portée de communication de l'émetteur qui ont reçu ce RTS savent qu'une communication va avoir lieu. Comme la durée de la communication est précisée dans le paquet RTS, ces mobiles peuvent alors se bloquer et s'empêcher d'émettre pendant toute cette période. Cette opération est réalisée grâce au NAV (Network Allocation Vector) qui stocke la valeur de cette durée et qui joue le rôle d'horloge. Le récepteur qui reçoit le RTS renvoie un paquet de contrôle CTS (Clear to Send) à tous ses voisins (même si il y a un nœud caché par rapport a l'émetteur du RTS) s'il n'est pas lui-même bloqué par son NAV. Le CTS a le même éffet que le RTS pour les mobiles`a portée de communication du récepteur. A la réception du CTS, l'émetteur sait que le médium a été réservé et qu'il peut donc émettre ses données.



ACK: (ACKnowledgement): acquittement NAV: Network Allocation Vector
DCF: (Distributed Coordination Function SIFS: (Short-Inter-Time Spacing)
DIFS (DCF Inter-Frame Spacing)

Figure 1.7 : Diagramme de séquence de transmission des trames

On note que ce mécanisme ne permet pas d'éviter les collisions d'une manière total comme montre la figure 1.8 car, des RTS peuvent être envoyé simultanément par de nombreux nœuds vers un nœud commun, cependant une collision de ce type ne gaspille pas autant de bande passante [1]

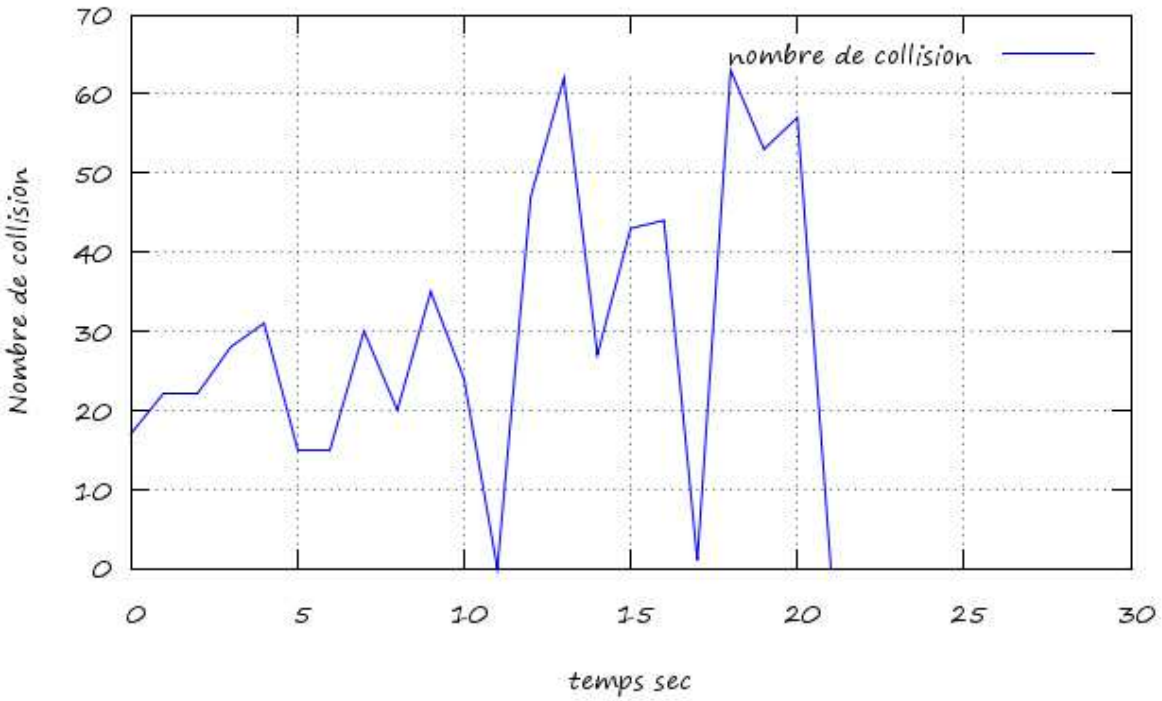


Figure 1.8 les collisions dans un réseau ad hoc

4. Les réseaux ad hoc

Un réseau de mobiles ad hoc, est un réseau constitué d'une collection d'entités mobiles interconnectées par une technologie sans fil formant un réseau *temporaire* sans l'aide de toute *infrastructure* ou de toute *administration centrale* [8]. Les nœuds mobiles d'un réseau ad hoc

peuvent communiquer directement entre eux s'ils sont à porté l'un de l'autre ou indirectement (en multi-saut) en utilisant d'autres nœuds mobiles comme relais intermédiaires pour transmettre leurs paquets vers une destination donnée. Seuls les nœuds mobiles eux-mêmes qui forment, d'une manière ad hoc une infrastructure du réseau. Ces réseaux s'organisent automatiquement de façon à être rapidement déployables et qui doivent pouvoir s'adapter aux conditions de propagation (canal variable, interférences,…), aux trafics et aux différents mouvements pouvant intervenir au sein des nœuds mobiles [12].

L'avantage des réseaux ad hoc est qu'ils peuvent couvrir une zone géographique importante, sans nécessiter d'un câblage ou d'une infrastructure préalablement installé notamment dans des endroits ou le câblage est difficile à mettre en œuvre, ainsi l'auto configuration permet à des nouveau mobiles d'intégrer facilement dans le réseau sans aucune configuration c'est le "plug and play", l'extension des services Internet hors la cellule d'un réseau de type wi-fi vers d'autres nœuds figure 1.8 aussi est un sujet d'actualité et un champs de recherches [25, 26], cela revient à la difficulté de gérer les protocoles de routage celles du monde IP et celles du monde ad hoc, ainsi les nœuds qui sont front avec Internet devient jouent le rôle des gatways donc il faut implémente d'autres spécifications dans ces nœuds afin de prise en charge la connectivité des autres nœuds, cependant le problème des batteries reste aussi un écueil contre le développement des ces réseaux notamment les points d'accès, même aussi le problème de routage

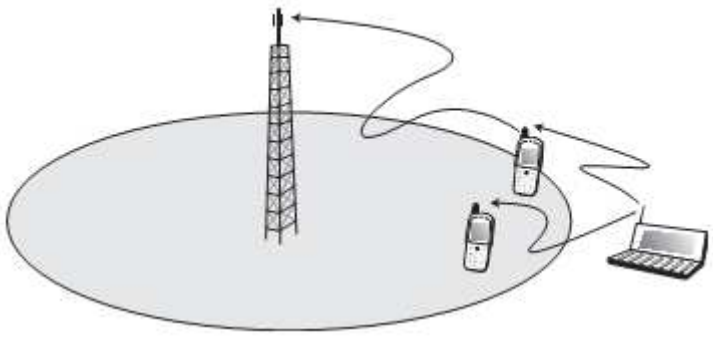


Figure 1.9 : Extension de couverture par un réseau ad-hoc

Le problème d'un réseau ad hoc est multicouche de la couche physique jusqu'à la couche application [16] :

- La couche physique doit s'adapter rapidement aux caractéristiques du lien.
- la couche MAC doit minimiser les collisions pendant le multi accès, en plus le problème des stations cachées.
- la couche réseau qui doit avoir un temps de convergence acceptable face aux différents changements dans la topologie du réseau.
- la couche transport : le manque d'une justification claire sur la cause des pertes des segments, implique une baisse massive du débit de transmission d'une façon aveugle.

4.1 Caractéristiques des réseaux ad hoc :

Comparant aux autres réseaux sans fil ou filaires, un réseau des mobiles ad hoc possède des caractéristiques particulières, celles-ci décrit dans un document Internet [9], qui sont :

- **absence d'infrastructure :** les réseaux ad hoc se distinguent des autres réseaux mobiles par l'absence d'infrastructure et de toute entité centralisée, chaque entité

mobile est responsable d'établir et de maintenir la connectivité de réseaux d'une manière continue, et aussi de participer au bon fonctionnement du réseau

- **Topologie dynamique** : les nœuds du réseau Manet sont libres de son mouvement ce qui résulte une topologie hautement dynamique et imprévisible, ainsi les liens entre les nœuds peuvent être symétrique ou asymétrique.

- **Multi-sauts** : Comme la portée des stations est limitée, il peut s'avérer nécessaire que des stations agissent en tant que pont intermédiaire pour transmettre un paquet d'une source vers une destination. Par conséquent, les nœuds d'un réseau MANET agissent en tant que routeur et relayent les paquets qu'ils reçoivent pour participer au routage multi-saut.
- **hétérogénéité des nœuds :** les nœuds d'un ad hoc peuvent correspondre à une multitude d'équipements: de l'ordinateur portable au PDA en passant par le téléphone mobile. Ces équipements ne disposent pas les mêmes propriétés physiques et logicielles, mais elles doivent pourtant interopérer pour établir un réseau commun.
- **contrainte d'énergie :** quelques ou touts les nœuds qui forment un réseau ad hoc sont équipés par des sources d'énergie autonomes comme les batteries, donc toute optimisation doit prendre ce paramètre en considération
- **sécurité physique limitée** : Les signaux étant diffusés, ils peuvent être écoutés par toute station mobile se trouvant dans la même zone de couverture. La confidentialité de certaines informations nécessite l'utilisation de mécanismes de sécurité adéquats.

4.2 Les applications des réseaux mobiles ad hoc :

Le champ d'application des réseaux est vaste et la recherche dans ce domaine est abondante, initialement, ces réseaux ont été construits dans une optique militaire, ils peuvent maintenant être utilisés dans des contextes divers : service urgence, secours, mesure climatique, conférences et les jeux interactives, la particularité du réseau ad hoc est qu'il n'a besoin d'aucune installation fixe, ceci lui permettant d'être rapide et facile à déployer. Les applications tactiques comme les opérations de secours, militaires ou d'explorations trouvent en ad hoc, le réseau idéal.

4.3 Modélisation d'un réseau ad hoc :

La topologie dynamique d'un réseau ad hoc peut être modélisé par un graphe orienté connexion $G_t(V_t, E_t)$ [17], d'où

- V_t : représente l'ensemble des sommets (terminaux mobiles) dans un instant *t*
- E_t : modélise l'ensemble des liens radio qui existent entre ces nœuds à un instant *t*
- $Nvi = \{vj \in V : (vi, vj) \in E \}$: ensemble de voisins d'un nœud.

La figure suivante représente un réseau ad hoc de cinq unités mobiles sous forme d'un graphe :

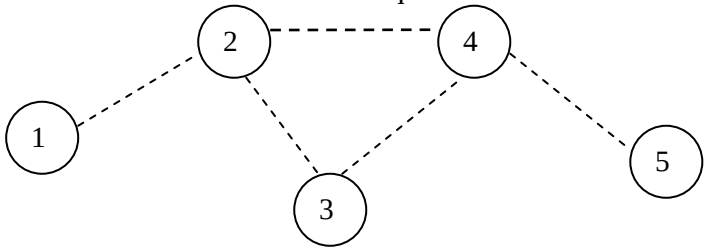


Figure 1.10 modélisation d'un réseau ad hoc

Si $e = (u, v) \in E_t$, cela veut dire que les nœuds u et v sont en mesure de communiquer directement à l'instant t

Cependant de nombreux problèmes dans les réseaux ad hoc (exploration du réseau, le routage, la gestion des ressources, etc.) peuvent être résoudre par des algorithmes de la théorie des graphes tel l'algorithme de plus court chemin, les chemins disjoints, les algorithmes qui détecte les boucles, ces algorithmes sont fortement appliqués dans la recherche de développement et de l'optimisation de ce type de réseaux

4.4 Le routage dans les réseaux ad hoc :

On défini le routage comme la manière à travers laquelle on fait transiter un paquet de donnée depuis un certain émetteur vers un destinataire précis, cette fonction est assuré par la couche réseau du modèle OSI. Inversement aux réseaux classiques où l'opération de routage est confiée à des équipements réseaux dédiés (routeurs), dans un réseau ad hoc chaque nœud contribue dans l'opération de routage, il joue le rôle d'un émetteur lorsqu il y a données à transmettre et le rôle un routeur lorsqu'il s'agit de transiter une information à certain destinataire le problème du routage est le premier challenge à résoudre dans un réseau ad hoc [13]

Les protocoles de routage élaborés et utiliser dans les réseaux Internet, base vecteur à distance ou état de lien (RIP, OSPF, IS- IS) [14] sont difficilement utilisables tels quels dans les réseaux ad hoc, cela est dû principalement de la mobilité des nœuds et de la topologie imprévisible. En effet, avec une topologie hautement dynamique et une grande partie des ressources radio très limitées. Des solutions adaptées aux caractéristiques des réseaux ad hoc est donc nécessaires, i.e. des solutions peu coûteuses en terme de bande passante et qui acheminent, si possible rapidement, les paquets à destination, quelque soient la dynamique du réseau.

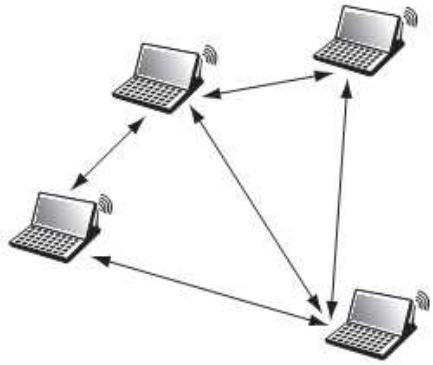


Figure 1.11 le routage d'information au sein d'un réseau ad hoc

Cependant la conception d'un protocole de routage pour les MANET il est désirable qu'il porte des propriétés qualitatives [9], [15] tel que :

- Trafic de contrôle "overhead" être minimal
- Un délai de bout en bout minimal
- Peu de perte des paquets
- Réactivité rapide au changement de la topologie, qui a un impact sur la perte des paquets
- Robuste contre les boucles

4.5 Classification :

Suivant la manière de création et de maintenance des routes lors de l'acheminement des données, les protocoles de routage peuvent être séparés en deux catégories [8], les protocoles proactifs et les protocoles réactifs. Les protocoles proactifs établissent les routes à l'avance en se basant sur l'échange périodique des tables de routage, alors que les protocoles réactifs cherchent les routes à la demande, une autre approche émerge dite “hybride” essai de combine les deux, afin de tiré les avantages de chacune.

4.5.1 Les protocoles proactifs :

Un protocole de routage proactif maintient régulièrement à jour des informations sur la topologie du réseau au niveau de chaque nœud, ces informations permettent à chaque mobile d’avoir rapidement la connaissance d’une route pour chaque destinataire du réseau. Ces protocoles dits “table-Driven” c'est-à-dire chaque nœud utilise sa propre table de routage pour aiguiller les données vers un voisin précis jusqu’ a atteindre le destinataire désiré.

Actuellement, les protocoles de routage proactifs les plus connus sont DSDV (Destination-Sequenced Distance-Vector) et OLSR (Optimized Link State Routing) qui sont devenus des RFC Expérimental, nous allons regarder un peu plus en détail le fonctionnement de ces deux protocoles.

4.5.1.1 Le protocole DSDV :

Le protocole DSDV “Destination Sequenced Distance Vector”, [18] est une optimisation du protocole de routage Internet RIP [14], dans ce protocole chaque nœud du réseau maintien une table de routage pour toutes les destinations possible dans le réseau ad hoc.

Chaque station diffuse l’ensemble de sa table de routage suivie d’un numéro pour dater l’information. Ce numéro est appelé numéro de séquence. A partir de deux numéros de séquence différents, il est possible de déterminer quelle information est la plus récente, une autre utilisation de ce numéro c’est d’éviter la formation des boucles de routage. Toute fois chaque nœud dans le réseau maintien une table de routage contenant :

- Toutes les destinations possibles dans le réseau
- Le noeud suivant, lequel on peut atteindre une telle destination
- Un numéro de séquence (SN) qui correspond à un nœud destination.

Afin de préserve l’actualisation des tables de routage et d’avoir un temps de convergence acceptable (temps entre un événement et le changement correspondant dans la table de routage) les mises à jour des tables de routage dans DSDV sont pilotées soit par le temps c'est-à-dire (périodique) ou bien par événement, s’il y a un changement dans la topologie du réseau, une particularité du protocole DSDV, comparant au protocole RIP est que la diffusion des paquets de mise à jour avec un métrique égale a un , ce paramètre permet à un nœud de ne rediffuse le paquet si le numéro de séquence inférieur à celui sauvé dans sa table

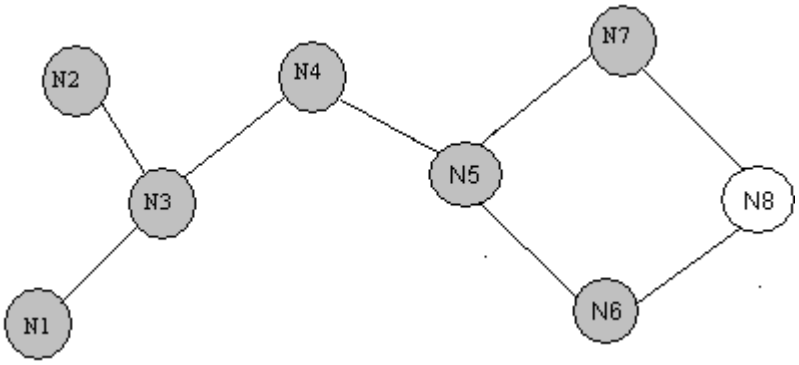


Figure 1.12 topologie du réseau

La table suivante rassemble les différentes informations stockées dans la table de routage du nœud N5

Destination	Nœud suivant	Métrique	N°-Séquence
N1	N4	3	N1005
N2	N4	3	N2003
N3	N4	2	N3555
N4	N4	1	N4665
N5	N5	0	N5658
N6	N6	1	N6898
N7	N7	1	N7564
N8	N7	0	N8125

Table de routage du nœud N5

L'actualisation des entrées de la table de routage se base sur le numéro de séquence. Elle s'effectue sur le schéma suivant : À la réception d'un paquet de mise à jour, une comparaison s'effectue entre le numéro de séquence sauvé et celui contenu dans le paquet. Si ce dernier est plus grand, il reflète alors une information plus fraîche et l'entrée est directement remplacée par celle du paquet. En cas d'égalité des numéros de séquence, la métrique du protocole étant le nombre de saut, seul la route formée par le plus petit nombre de saut sera retenue.

Afin de préserve la consommation de la bande passante, DSDV défini deux types de mis à jour des tables.

- Mise à jour complète : qui n'est rien autre que la mise à jour périodique, où le nœud transmet la totalité de sa table de routage vers ses voisins.
- Mise à jour incrémentale : cette mise à jour n'est faite qu'en cas d'événements (Apparition d'un nouveau voisin, disparition d'un nœud ...etc.), et dans ce cas il n'y a que l'entrée concernant le nœud en question dans la table de routage qui change.

4.5.1.2 Le protocole OLSR :

Le protocole Optimized Link State Routing (OLSR), standardisé en 2003 par l'IETF dans le document Internet [RFC 3626] [20]. OLSR est conçu spécialement pour des réseaux ad hoc qui se caractérisent par une haute densité et une forte mobilité, comme il est de nature proactif, chaque nœud échange régulièrement avec d'autres nœuds l'information sur la topologie du réseau.

OLSR considère comme une optimisation des protocoles à état de liens, en évitant la l'inondation total du réseau, il utilise un mécanisme d'inondation intelligent, qui résulte une réduction considérable du nombre de retransmissions des paquets de contrôle et économise une grande partie des ressources réseau. La notion clé du protocole OLSR est les nœuds MPR (Multi-Point Relay), qui sont des nœuds ont la particularité d'être les meilleurs points de passage pour atteindre l'ensemble des nœuds lors d'un processus d'inondation sans diffuser tous azimuts, les nœuds qui ne sont pas déclarés comme MPR n'ont pas le droit de retransmet les paquets de contrôle dans le réseau, voir (figure1.7).

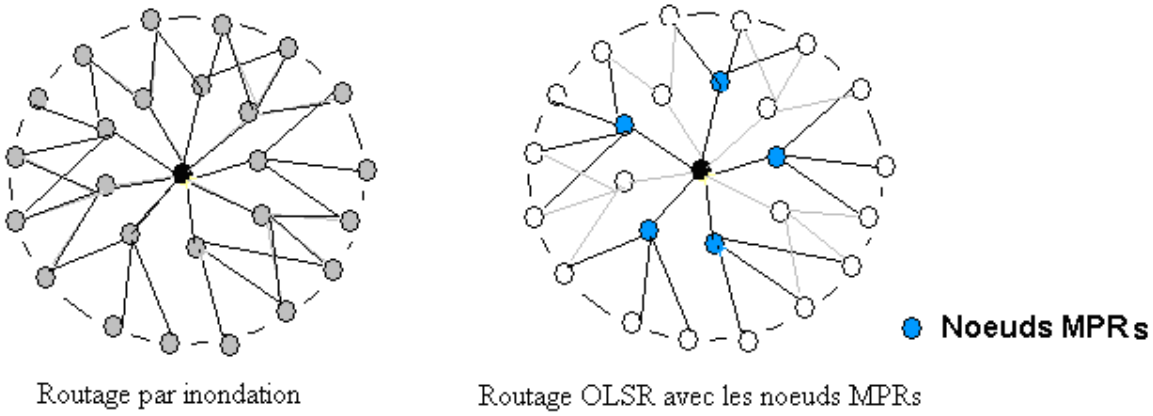


Figure 1.13 routage OLSR

L'élection des nœuds MPR se fait comme suite : chaque nœud détecte l'ensemble de ces voisins grâce à des messages "HELLO" ce message diffuse à l'ensemble des voisins qui situent à une distance égale à deux sauts, ceci permet à un nœud de construire une base de connaissance sur ces voisins (symétrique, asymétrique ou MPR) puis chaque nœud choisi parmi les voisins ses propre nœuds qui opèrent comme des MPRs, et qui peuvent couvrir tous les nœuds qui situent à une distance égale à deux sauts, cependant l'ensemble des MPRs est recalculé dans les deux cas suivants :

- Un changement de voisinage : Une liaison symétrique est rompue ou un nouveau voisin est détecté.
- Un changement dans le voisinage à deux sauts : avec les mêmes causes.

4. 5 .2 Les protocoles réactifs :

Sont des protocoles dans lesquels la mise à jour ou le contrôle des routes se fait à la demande, il n'utilise donc la bande passante que lorsqu'il en a besoin, puisqu'il ne maintien pas à jours d'information sur le réseau quand ce n'est pas nécessaire. L'établissement d'un chemin entre deux nœuds distinct ne fait que s'il y a un échange de données entre eux c'est-à-dire lorsqu'une source veut transmettre des paquet de données vers une destination, donc le temps de latence plus ou moins long comparé au protocoles proactif .ces protocoles reposent sur deux mécanisme vitaux qui sont

- La *recherche* de route (découverte)
- La *maintenance* de la route (durant la communication) : due de la rupture des liens

Actuellement, les protocoles de routage réactifs les plus connus sont DSR (Dynamiq Source Routing), AODV (ad hoc On-Demand Destination Vector), qui devenus des RFC de IETF

4.5.2.1 Le protocole DSR :

Le protocole Dynamic Source Routing (DSR) décrit dans [21], qui a été standardisé en 2007 [RFC 4728], basé sur l'utilisation du technique "routage à la source", dans cette technique, une source des données détermine la séquence complète des nœuds à travers lesquelles, les paquets des données seront arrivent vers le destinataire.

Données	DST	N_N	·····	N_3	N_2	N_1

Figure 1.14. : Format générale d'un paquet DSR

Parmi les avantages de ce protocole est l'absence total des boucles de routage, car le chemin source / destination fait partie des paquets des données figure1.12 cependant protocole DSR se compose de deux mécanismes complémentaires qui sont :

- La découverte de la route

Quand une source veut transmettre des données vers une destinataire, elle commence par une vérification dans sa table route_cache, afin de trouver une route valide vers le destinataire, si c'est pas le cas, la source initié un mécanisme de découverte de la route par la diffusion d'un paquet RREQ vers ses voisins, si l'un des voisins reçu ce paquet il vérifie si cet requête elle destiné pour lui ou non, pour le premier cas, il envoie un répone_route RREP vers la source après qu'il copies les information de routage accumulent dans le paquets RREQ, sinon (ce n'est pas le destinataire) ,il vérifie s'il y a une route disponible dans sa table route_cache vers cette destination, si ce voisin ni un destinataire et n'avoir aucune route disponible ,il ajoute son adresse dans le RREQ, et rediffuse ce paquet vers ses voisins (figure1.9)

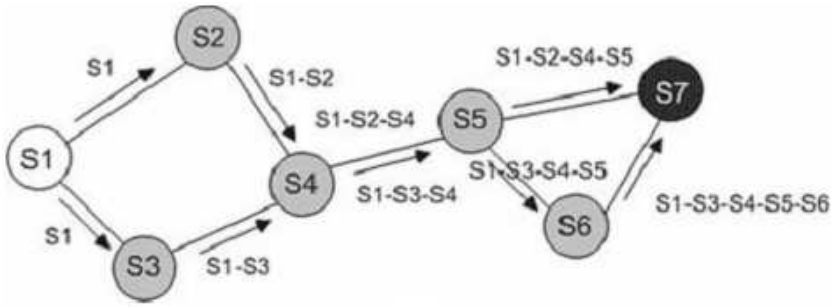


Figure 1.15 : Le processus de découverte de la route dans DSR

Ce processus continue jusqu'à le paquet atteindre le nœud destinataire .quand une source recevoir un paquet RREP elle commence l'envoie des données à travers la route spécifié dans le RREP .si plusieurs chemins sont découverte (plusieurs RREQ arrivent) le destinataire choisis un chemin qui est le plus court.

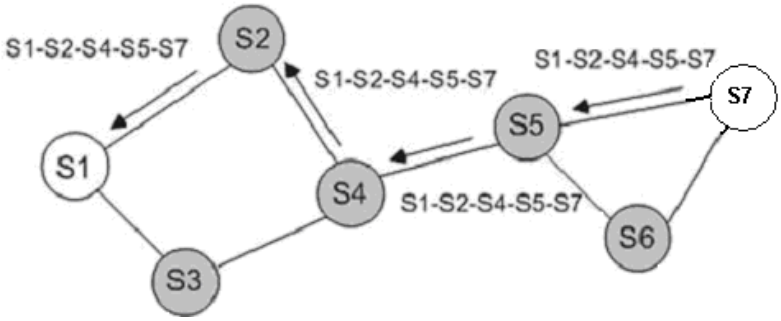


Figure 1.16 la réponse de la route RREP

Le deuxième mécanisme c'est "la maintenance de la route" qui s'exécute aussi à la demande c'est-à-dire le transfert des données est active sur cette route, avec ce mécanisme la source est capable de détecte toute rupture dans le chemin, quand un nœud détecte une rupture d'un lien, grâce à sa couche MAC. Si au bout d'un certain nombre d'émissions aucun acquittement n'est reçu, le chemin est considéré non valide. Un nœud détectant la rupture prévient l'ensemble des sources avec un paquet d'erreur (Route Error). A la réception d'un tel paquet, la source détermine une nouvelle route si aucune autre n'est disponible.

4.5.2.2 Le protocole AODV :

Le protocole AODV *"Ad-hoc On-Demand Distance vector"* est décrit dans un document de IETF [RFC 3561], [22], AODV peut être considéré comme une combinaison des deux protocoles DSDV et DSR, car il détient de DSR son mécanisme de découverte et de maintenance de routes, et de DSDV, son routage distribué en gardant une table de routage au niveau de chaque nœud, ainsi les jours des tables de routage. La spécification du protocole AODV pour le routage des données repose sur les mécanismes suivants :

a) La découverte de la route dans AODV:

Le processus de la découverte de la route dans AODV se déroule comme suit :

Lorsque une source désire faire un échange des données avec un noeud, d'abord après une vérification dans sa table cache, elle diffuse à travers le réseau une requête RREQ pour la structure de RREQ (voir figure 1.15) afin d'obtenir d'une route vers le destinataire, lorsque un nœud intermédiaire reçoit cette requête, elle génère une réponse sur la route avec un paquet RREP dans les deux cas suivantes :

1. il même le bon destinataire
2. possède une route vers le destinataire

RREQ
RREQ ID
Adresse Source
Adresse Destinataire
Nombre de Sauts
Num-seq Source
Num-seq destinataire

RREP
Adresse Source
Adresse Destinataire
Num-seq destinataire
Nombre de Sauts
Temps expire

Table de routage
Adresse destinataire
Saut suivant
Nombre de saut
Num-seq destinataire
Liste voisin
Temps expire

Figure 1.17 : Format général d'une requête RREQ, vs RREP table de routage

Si c'est pas les cas, elle diffuse la requête vers ses voisin en incrémente le nombre de sauts jusqu' arrive vers le destinataire, cependant si un nœud intermédiaire reçoit plusieurs copies de la requête RREQ avec le même couple "RREQ_ID, l'adresse source", il la rejette et ne la diffuse pas.

b) Création du chemin inverse :

Eventuellement, une requête RREQ arrive à un nœud (possible lui même le destinataire) déjà possède une route vers le destinataire, d'abord avant de retourner une réponse, il fait une vérification en comparant le numéro de séquence correspond au destinataire dans le RREQ avec celle qui existe correspond dans sa table de routage, si le nombre est plus grand que celui qui déjà stocké dans la table de routage, le nœud *ne doit pas* répondre à la requête avec la route déjà enregistré dans la table, mais il rediffuse la requête, il retourne en arrière une réponse "RREP" vers l'un des voisins qui fait l'émission de la requête RREQ. Cette réponse, et de la même manière ce nœud faire aiguiller la réponse vers l'émetteur de la requête ce processus continue jusqu'à la réponse arrive à la source.

Une fois la source reçoit une réponse sur la route avec RREP voir figure 1.16, elle commence le transfert des données en suivant un routage saut-par-saut, si ultérieurement elle reçoit une autre RREP avec un nombre de saut plus petit elle bascule change vers nouvelle route après une mis a jours de sa table de routage

Précisons que le protocole AODV ne supporte que les liens symétriques dans la construction des chemins inverses; c'est-à-dire que lorsqu'un nœud intermédiaire transmet le paquet RREQ à un voisin, il procède la à sauvegarde de l'identificateur du nœud à partir duquel la première copie de la requête est reçue. Ce chemin inverse sera traversé par le paquet RREP, et de cette façon tous les nœuds appartenant au chemin retour modifieront leurs tables de routage en fonction du paquet réponse de route.

La gestion des tables de routage :

La méthode de routage de AODV est inspirée du DSDV, elle base sur un routage distribué sur les différents nœuds du réseau, la structure da la table est montrée dans la figure 1.15, l'intérêt de cette table, a l'adjonction de l'opération de routage un nœud intermédiaire peut l'utiliser pour répondre à une requête RREQ, sans la diffusée vers d'autres nœuds du réseau ou vers le destinataire eu même

c) La maintenance de la route :

L'établissement de la route, AODV détient un mécanisme lui permet de contrôler la validité de la route ou toute rupture possible durant la période de l'échange des données

d) La gestion de la connectivité locale :

La gestion des routes consistantes et la connectivité locale est appliquée par les nœuds de la manière suivante : chaque nœud fait partie d'une route active, émet périodiquement vers ses voisins un paquet nommé "HELLO" (vous êtes là?) qui se compose d'un <identificateur du nœud, numéro de séquence> et qui dote d'un TTL égale à 1 pour éviter la propagation du paquet vers des nœuds hors les voisins, à la confirmation par un message "HELLO-ACK" les nœuds apprennent la présence des nœuds voisins, cependant cette connectivité est modifiée dans les cas suivants : un nœud reçoit un paquet Hello

transmis par un nouveau voisin ou un nœud ne reçoit plus d'acquittement après l'émission de trois message "hello" successif.

La principale différence entre les deux approches réside dans la technique de stockage des informations de routage. Dans AODV, chaque noeud connaît, pour chaque destination avec laquelle il communique le saut suivant sur la route alors que dans DSR, la source stocke toute les informations et inclut la route dans l'entête des paquets de données.

L'avantage principal du protocole DSR par rapport AODV est leur simplicité d'implémentation. Dans DSR les nœuds intermédiaires n'ont pas besoin de maintenir une table de routage (le cas du AODV), cependant avec DSR plus surcharge "overhead" impliqué dans le routage des paquets de données, cela revient parce que dans DSR la route entière doit être spécifié dans l'entête du paquet, à l'inverse AODV il maintien un routage distribué saut-par-saut.

4. 5. 3 Les protocoles hybride

Le principe des algorithmes hybrides est de combiner les deux approches afin de tirer parti des avantages des deux approches. Ces protocoles basés soit sur le principe de diviser le réseau Manet en zones [28], ou de créer un sorte de backbone, afin de préserve la consommation de la bande passante en réduisant l'espace proactive d'un nœud, dans l'autre cas il minimise l'inondation de tous le réseau par des paquets de type RREQ, et réduire le temps de découverte de la route s'il concerne d'un protocole sur demande. Ce type d'algorithme s'inspire du comportement humain, c'est-à-dire que nous avons une bonne connaissance du quartier où l'on habite, mais plus on s'en éloigne, plus on ne connaît que les axes pour atteindre notre lieu de destination, et pas ce qui l'entoure. Plusieurs protocoles appartient à cette famille citons (ZRP, ZHLS, DST,….) on limite notre description au protocole ZRP.

4.5.3.1 Le protocole ZRP

Le protocole ZRP (Zone Routing Protocol) [28] est un modèle hybride entre un schéma proactif et un schéma réactif, un noeud limite la procédure proactive uniquement aux nœuds voisins à *h* sauts, alors il utilise un routage réactif hors cette zone, comme son indique, le protocole ZRP est basé sur le concept de zone, où chaque nœud définie son propre zone. Une zone de routage est définie pour chaque nœud et incluse les terminaux qui sont à une distance minimale en terme de sauts du nœud en question (figure 1.8). La valeur du rayon de zone détermine la performance du protocole, en général, les réseaux mobiles doivent fixer cette variable à la valeur la plus petite possible, alors que pour un réseau faible mobilité, elle prendra une valeur plus grande. De même, dans des réseaux très actifs (requêtes fréquentes), le rayon de zone doit être plus grand contrairement aux réseaux moins actifs. Dans ZRP nœuds deux types de nœuds définis frontières sont ceux pour lesquels la distance minimum qui les sépare du nœud considéré est exactement égale au rayon de zone, et nœuds intérieurs

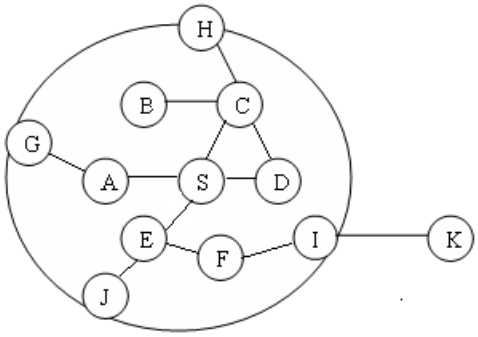


Figure 1.16 : Exemple d'un routage à zone avec *h*= 2

Exemple d'un routage basé sur la zone de routage d'un nœud S,cette zone incluse les nœuds,de A-I, mais pas le nœud K. Le diamètre est identifie par le nombre de sauts et non pas par la distance physique

Car la zone de routage pour chaque nœud est déterminée, ceci peut réduit le trafic quand la découverte de la route est indispensable, au lieu d'utiliser une diffusion "broadcasting", ZRP utilise une autre méthode appelée le "bordercasting" qui est un processus d'émission des datagrammes IP (RFC-0791) à partir d'un nœud vers tous ses nœuds périphériques. Bordercasting peut être implémenté soit à travers une émission IP unicast classique soit à travers une émission multicast (Distance Vector Multicast Protocol – RFC 1075). L'approche multicast est évidemment préférable afin de réduire la quantité de trafic dans l'air.

- **Mécanisme de Routage**

Lorsque une source veut transmettre un paquet, d'abord elle vérifie l'existence de cette destination dans sa table de routage, si cette destination déjà existe dans sa zone locale, si c'est le cas, les données routent proactivement vers le destinataire, si c'est le cas le nœud source envoie paquet de découverte de la route vers les nœuds périphériques, si l'un des périphériques connaît une route, il réponde par l'envoie un RREP en retour à la source indiquant le chemin à emprunter pour atteindre la destination, si ce n'est pas le cas, les nœuds périphériques font suivre la demande à leurs propres nœuds périphériques qui à leur tour effectuent la même procédure.

5. Les modèles de mobilité :

La mobilité dans les réseaux ad hoc est un point délicat à traiter, cela est due de la nature des réseaux ad hoc et la topologie imprédictible. Définir un modèle permet de prévoir le déplacement des nœuds et d'estimer la topologie du réseau, ainsi que peut aider à une convergence vers la réalité, de nombreux modèles a été proposés [9], [29].Chacun a des spécificites propres, liées à un comportement et des objectifs recherchés. Il peut s'agir de :

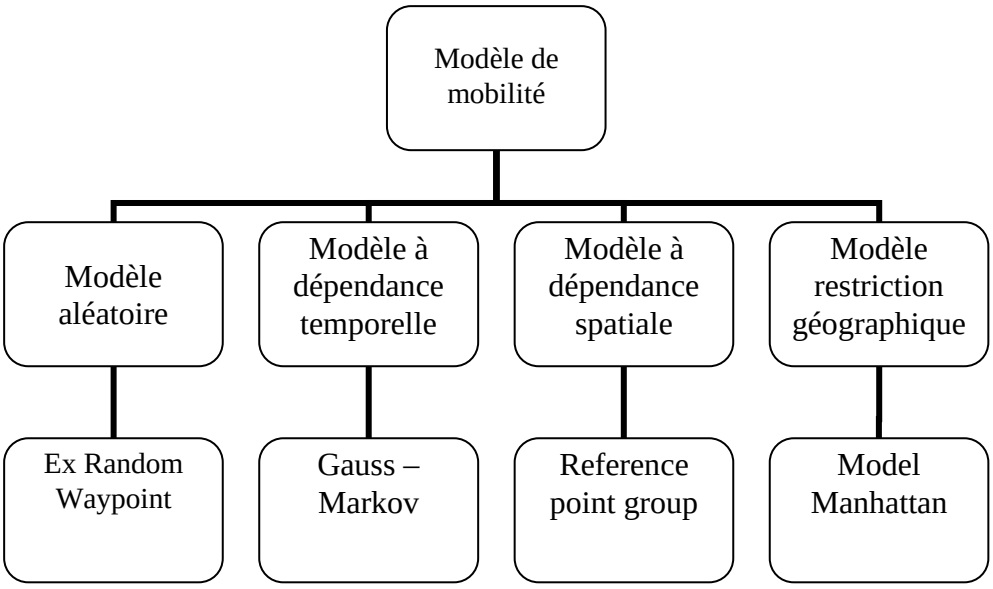


Figure 1.19 : les différents modèles de mobilité

- Modèle aléatoire : les nœuds se déplacent d'une manière libre sans contraintes temporelle ou spatiale
- Dépendance temporelle : la vitesse d'un nœud à un moment donné est corrélée avec sa vitesse dans le passé
- Dépendance spatiale : les nœuds se déplacent en groupe, et ils s'influent sur le déplacement des autres nœuds à proximité
- Restriction géographique : un nœud ne peut franchir une zone ou doit suivre un axe.

On a choisit pour la simulation le modèle RWP Random Waypoint, un modèle qui est largement utilisé pour simuler des réseaux de type ad hoc [8], ainsi sa spécification est intégré dans les environnements de simulation d'OPNET et NS-2

Dans RWP les noeuds sont uniformément répartis dans un espace de mobilité, un nœud alterne les périodes de mouvement et d'immobilité, chaque nœuds choisit et déplace vers une destination D_1 sur la surface de simulation avec une vitesse V_1 distribué uniformément dans l'intervalle [V_{min}, V_{max}] (V_{max} la vitesse maximale qui est indépendante de l'un de l'autre), dés que le arrive à la destination D_1 faire une pause pendant un temps T_{pause}, puis choisi au hasard une autre position D_2 avec une vitesse V_2, à l'arrivé il effectue à nouveau un pause, et ainsi de suite

Deux paramètres clés dans le modèle RWP, V_{max} et T_{pause} qui identifient le comportement de la mobilité d'un nœud et la stabilité de la topologie du réseau. Si V_{max} est plus petite et T_{pause} est plus long la topologie est relativement stable, en revanche si la vitesse V_{max} est plus grande et le T_{pause} est plus court la topologie hautement dynamique. Selon ces deux paramètres RWP peut génère plusieurs scénario de mobilité. L'inconvénient de ce modèle il ne traite pas le cas où il y a une dépendance entre un groupe de nœuds (dépendance temporelle ou spatiale), qui a un impact sur les résultat de la simulation .

6. études par simulation des protocoles AODV, DSR et OLSR :

Dans cette partie on fait une simulation sur les performances des protocoles familles réactif (AODV, DSR) et proactif (OLSR). On utilise pour notre étude le simulateur (OPNET Modeler v 14.5) Optimized Network Engineering Tool avec le modèle de mobilité "Random Waypoint", la table suivant récapitule les différents paramètres de l'environnement OPNET et le modèle RWP

modèle de mobilité	Random waypoint
vitesse	uniforme [0, 25] et m/sec
nombre de nœuds	10
Nœuds destination	Aléatoire
Standard	IEEE 802.11
Débit	11 Mbits /sec
Surface	900 m²
Temps de simulation	400s

Les paramètres de performance :

Pour l'évaluation des performances de chaque protocole de routage on a choisis les paramètres suivants :

- **Le délai :** est le temps (exprimé en seconde) écoule par un paquet d'une source vers la destination, il est exprime par la relation suivante :

$$D_{end-end} = N[D_{trans} + Dp_{rop} + D_{proc}] \text{.....(1)}$$

$D_{end-end}$: délai bout en bout
D_{trans} : délai de Transmission
D_{prop} : délai de Propagation
D_{proc} : délai de moyen de traitement
N : le nombre des noeuds traversé par un paquet

- **La charge du réseau** : représente la charge total en bit/sec soumis à la couche physique par toutes les couches hautes par tous les nœuds du réseau, ce paramètre influe fortement sur la vie du réseau ad hoc

- **Throughput (gain de performance)**: c'est le débit du réseau exprimé en (bit/sec ou byte/sec), certains facteurs influent sur le débit tel que le changement de la topologie la bande disponible et l'énergie des nœuds, ce paramètre est représenté par l'équation suivante :

$$débit = \frac{nombre\ \ de\ \ paquets\ \ délivré * taille\ \ du\ \ paquet}{durée\ \ totl\ \ de\ \ la\ \ simulation}$$

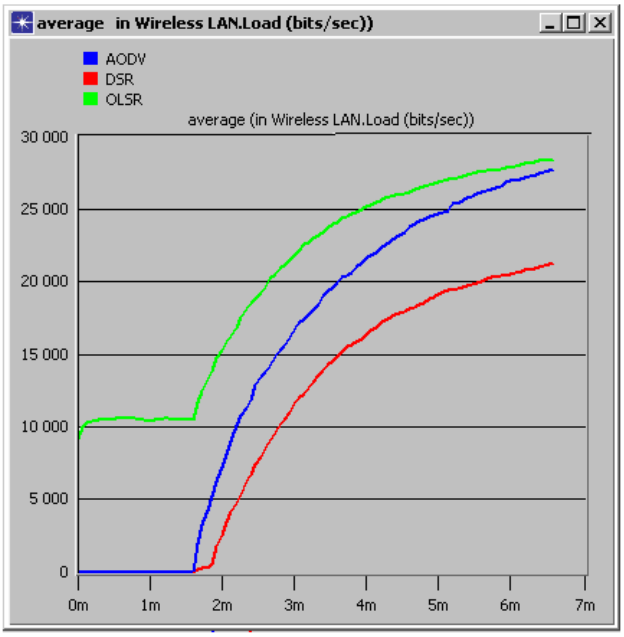


Figure 1.20 : la charge moyenne du réseau

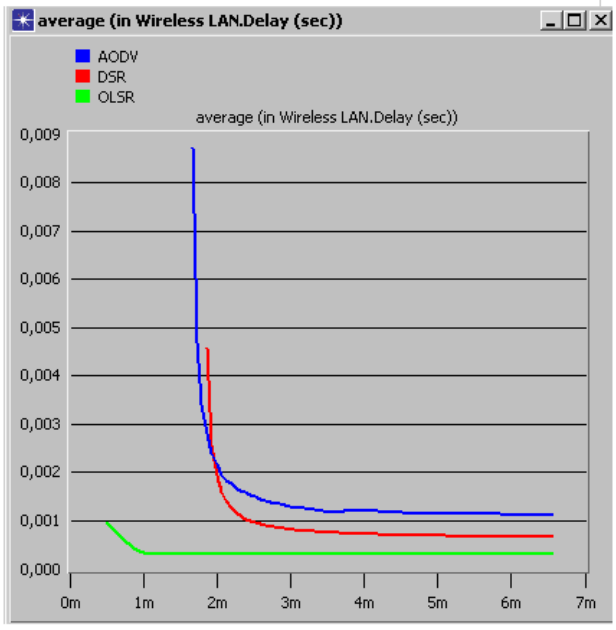


Figure 1.21 : le délai moyen du réseau

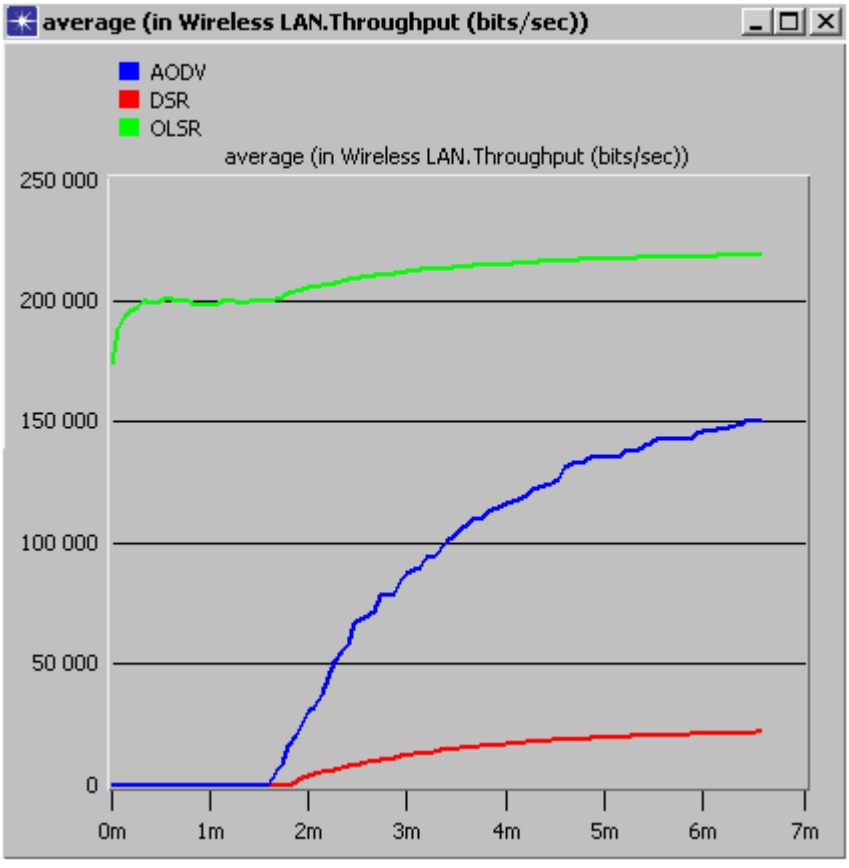


Figure 1.21 throughput moyen du réseau

Discussion :

D'après les résultats de la simulation, nous avons remarqué que :

En terme de la charge du réseau : OLSR génère plus de charge que les autres protocoles, à cause de l'aspect proactif du protocole, où les chemins entre les différents nœuds sont crée à l'avance. Cette charge influe grandement sur l'énergie des nœuds explicitement sur la vie total du réseau, donc le DSR est apparu le meilleur car il génère moins de la charge dans le réseau

En terme du délai : du de l'aspect proactif, où les nœuds s'identifient d'échange entre eux, le protocole OLSR meilleurs que DSR et AODV. Le protocole AODV c'est avéré le plus médiocre par apport aux autres protocoles, du fait qu'il ne supporte que les liens symétriques pendant la phase de découverte de la route ce influe sur le délai de transfert bout en bout.

En terme de throughput, on voit que OLSR plus performant que les autres comme nous avons mentionné cela revient à l'aspect proactif du protocole et la réactivité rapide aux différents changements dans la topologie du réseau, pour le DSR car il utilise un routage à la source c'est-à-dire que les informations de routage son incluses dans l'entête du paquet, cette technique influe sur fortement sur le volume des données brutes reçu par le destinataire.

En conclusion, AODV représente le protocole le plus équilibré en terme de délai, charge et débit selon les différents paramètres qu'on a choisis pour la simulation

7. Conclusion :

Nous commençons ce chapitre par une généralisation sur les différents modèles réseau existants : TCP/IP et OSI ceci nous permet de comprendre le problème posé ainsi la solution proposée dans les chapitres qui suit, puis nous avons présenté les réseaux IEEE 802.11, et particulièrement leur mode ad hoc avec leurs caractéristiques (absence infrastructure, topologie dynamique, et leurs contraintes.

Dans l'étude des protocoles de routage, nous présentons les trois classes de protocoles de routages : Proactifs, Réactifs et hybrides, ainsi que les politiques et les méthodes d'acheminement sur lesquelles ils reposent. Par la suite nous avons donnés des exemples de protocole pour chacune des trois classes avec une étude exhaustive sur le protocole AODV qui fait par la suite l'objet de notre étude, puis nous avons fait une comparaison par simulation entre ces différent protocoles, les différents métriques choisis pour l'étude sont : la charge, le délai et le débit, nous avons vu que chacun des protocoles ayant des puissants et des faiblesses nous concluons que le protocole AODV fait un compromis entre ces protocoles

Référence :

[1] G.Pujolle "*les réseaux* ", eyrolles édition 2008

[2] C. Servin “RÉSEAUX ET TÉLÉCOMS” édition Dunod 2003

[3] A. Tanembum “Computer Networks” edition Prentice Hall, 2003

[4] W.Stallings “Data and computer communication” sixième édition prentice hall 2008

[5] M. Gast “802.11 Wireless Networks: The Definitive Guide” edition O'Reilly 2002

[6] W.Stallings “Wireless communication and networks” deuxième edition Prentice Hall 2005

[7] Crow and al “IEEE 802.11 Wireless Local Area Networks” IEEE Communication 1997

[8] S. Sesay, Z.Yang and J. He “A survey on mobile ad hoc Wireless Network” Asian network for scientific information 2004 ISSN 1682-6027

[9] S. Corson J. Macker “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations” RFC 2501, IETF 1999

[10] B.O’Hara “*The IEEE 802.11 Handbook, a designer’s companion*” IEEE press 1999

[11] S. Misra , I.Woungang ″Guide to wireless ad-hoc″ edition Springer 2008.

[12] J.Wu, I. Stojmenovic “Ad hoc Networks” journal IEEE février 2004 Page 29-31

[13] N. Milanovic et al “Routing and Security in Mobile Ad Hoc Networks” journal IEEE février 2004 Page 61-64

[14] G. RUBINO, L TOUTAIN “Routage dans les réseaux Internet” article techniques de l’ingénieur, document H1 428

[15] S. Naski “Performance of Ad Hoc Routing Protocols: Characteristics and Comparison” Seminar on networking, April 2004

[16] Li, X. and Bao-yu, Z., “Study on Cross-layer Design and Power Conservation in Ad Hoc Network,” Parallel and Distributed Computing, Applications and Technologies, PDCAT, pp. 324-328., 27-29 Aug 2003

[17] C. Bettstetter “On the Connectivity of Ad Hoc Networks” the British Computer Society Vol. 47 No. 4, 2003

[18] C.E. Perkins and P. Bhagwat, “Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers,” in Proc. ACM SIGCOMM 94, London, UK, Oct. 1994, pp. 234-244

[19] A.H AbdRahman , Z. A. Zukarnain “Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks” European Journal of Scientific Research (2009), pp.566-576

[20] T. Clausen, P. Jacquet “Optimized Link State Routing Protocol (OLSR)” RFC 3626, IETF 2003

[21] D. Johnson, Y. Hu and D.Maltz. “*The dynamic source routing for mobile ad-hoc Networks*” RFC 4728, IETF 2007

[22] C.Perkins , E. Belding-Royer ”*Ad-hoc on-demand distance vector (AODV) routing*” . RFC 3561, IETF 2003

[25] F M. Abduljalil and S. Bodhe "A survey of integrating IP mobility protocols and mobile ad hoc networks" IEEE Communications Surveys & Tutorials • 1st Quarter 2007

[26] P. M. Ruiz and A. G. Skarmeta "Internet Connectivity for Mobile Ad Hoc Networks: Solutions and Challenges" IEEE Communications Magazine • October 2005

[27] S. Basagni et al "Mobile ad hoc networking" IEEE PRESS 2004

[28] M.R. Pearlman, Z. J. Haas "Determining the Optimal Configuration for the Zone Routing Protocol" journal IEEE 1999, page 1395-1414

[29] N. Cooper, N. Meghanathan "*Impact of Mobility Models on Multi-path Routing in Mobile Ad Hoc Networks* ˝ International Journal of Computer Networks & Communications, Vol. 2, No. 1, January 2010.

[30] U.T. Nguyen and X. Xiong, ''Rate-adaptive Multicast in Mobile Ad-hoc Networks'', Department of Computer Science and Engineering York University Toronto, Canada

Chapitre 2 :

Le routage multichemin dans les réseaux ad hoc

1. Introduction

Un réseau mobile ad hoc est un réseau constitué d'un ensemble de nœuds mobiles, qui fonctionne sans l'existence d'une infrastructure ou d'une administration centrale, ce type de réseaux est caractérisé par l'auto-configuration, l'auto-organisation et l'auto-maintenance.

Les nœuds mobiles d'un Manet peuvent communiquer directement entre eux s'ils sont à porté l'un de l'autre (pair-à-pair) ou indirectement (en multi-hop) en utilisant d'autres nœuds mobiles comme relais intermédiaires pour transmettre leurs paquets vers une destination donnée. Ainsi, la conception d'un protocole de routage qui prend en charge ces caractéristiques est essentielle, pour cela plusieurs protocoles de routages ont été proposés, ces protocoles de routage sont de type proactif, réactif ou hybride.

Dans les protocoles proactifs, la mise à jour des tables de routage se fait périodiquement, provoquant ainsi un trafic important qui est dû principalement à cet échange d'information, ce genre de routage ne convient pas aux réseaux Manet.

Pour pallier aux limitations de ces protocoles d'autres protocoles de nature réactif ont été proposés tels que : DSR et AODV, dans ces protocoles le chemin entre la source et la destination, est tracé lorsqu'il y a un besoin réel de transfert d'information. Leur fonctionnement repose sur les deux mécanismes suivants:

- La découverte de la route : une source l'utilise afin d'atteindre la destination.
- La maintenance de la route : pour détecter et rectifier tout changement dans la topologie du réseau.

Une fois tous les chemins sont découverts, la source choisit celui ayant le plus court chemin pour aiguiller ses paquets d'information. Mais dans certains cas, l'algorithme basé sur le plus court chemin ne présente pas le meilleur choix, puisque les nœuds qui se situent au centre du réseau peuvent transporter un trafic important comparativement aux nœuds qui sont situés au périmètre du réseau [1]. Ce qui peut engendrer une situation de congestion sur ces nœuds provoquant ainsi une dégradation importante des performances du réseau en termes de délai et de débit.

Une des limitations des protocoles *unipath* est qu'ils construisent une seule route entre la source et la destination. Ainsi, lorsqu'il y a une rupture de connexion dans cette route, les nœuds intermédiaires suppriment les paquets de données car ils ne disposent pas d'aucun chemin alternatif. Pour reprendre la transmission, la source sera obligée de relancer une nouvelle découverte de route ce qui influencera sur délai de bout en bout.

Le traitement de la forte mobilité des nœuds demande un protocole ayant une grande flexibilité qui s'adapte rapidement aux changements de la topologie du réseau, et une rapidité des recouvrements des chemins. Une telle flexibilité peut être achevée par l'utilisation d'une solution dite protocoles de routage multichemin qui créent un niveau de redondance entre le couple source /destination. Lorsqu'il y a un échec d'une route, les autres routes restent disponibles, donc la commutation du transfert vers un autre chemin faire d'une manière systématique L'idée de router les paquets sur Multichemin est déjà utilisée dans les réseaux IP à commutation de paquet face aux limitations des réseaux à commutation de circuit [2].

2. Avantages des protocoles de routage multichemins

La plupart des protocoles de routage multichemin proposés sont de types réactifs, vu que les protocoles proactifs sont sensés réagir implicitement à chaque changement topologique. Ces protocoles offrent ainsi un certain nombre d'avantages [3], par rapport aux protocoles *unipath* qui peuvent être résumés comme suit :

- Augmentation de la fiabilité : le routage multichemin offre à l'émetteur plusieurs routes à la fois pour atteindre un destinataire donné, ce qui permet d'améliorer la performance et la fiabilité du réseau, lorsque un lien est rompu autres routes restent disponibles, cela s'effectue sans lancer un nouveau processus de découverte de la route. Une autre façon de garantir la fiabilité c'est de transmettre plusieurs copies identiques sur des chemins différents [9].
- Augmentation sur le nombre globale des paquets reçu : comparant aux protocole mono chemin, la durée de récupération de transfert pour les multichemin après une rupture, assez rapide ce qui influe grandement sur le nombre total de paquets reçu par un destinataire (voir figure 2.4).
- Equilibrage de la charge : "load Balancing" c'est la distribution du trafic sur des chemins différents, cette distribution conduit à une utilisation équitable des ressources réseau [1], toute en évitant la compensation du trafic sur un chemin unique.
- Maximisation la vie du réseau : la vie d'un réseau ad hoc, dépend implicitement de l'énergie des nœuds, la répartition du trafic sur différent routes conserve d'énergie d'un certains nœuds, ce qui prolonge la vie des nœuds d'un réseau ad hoc
- Sécurité : la vulnérabilité est l'une des problèmes de sécurité dans les réseaux ad hoc, la dispersion des données sur des différent chemins empêche les attaques réseau de type "*Man-in-the-middle*"[12].

3. Impact de la longueur sur la rupture du chemin:

La possibilité d'une coupure de chemin entre deux nœuds, augmente avec la longueur du chemin : étant donnée une probabilité de coupure de lien *prl*, la probabilité d'une coupure de chemin ***Pb*** pour un chemin de la longueur ***k*** peut être simplement obtenue par $Pb = 1-(1- prl)^{K}$ [4]. La Figure 2.1 montre la variation de la probabilité ***Pb*** avec la longueur de chemin pour $prl = 0.1$

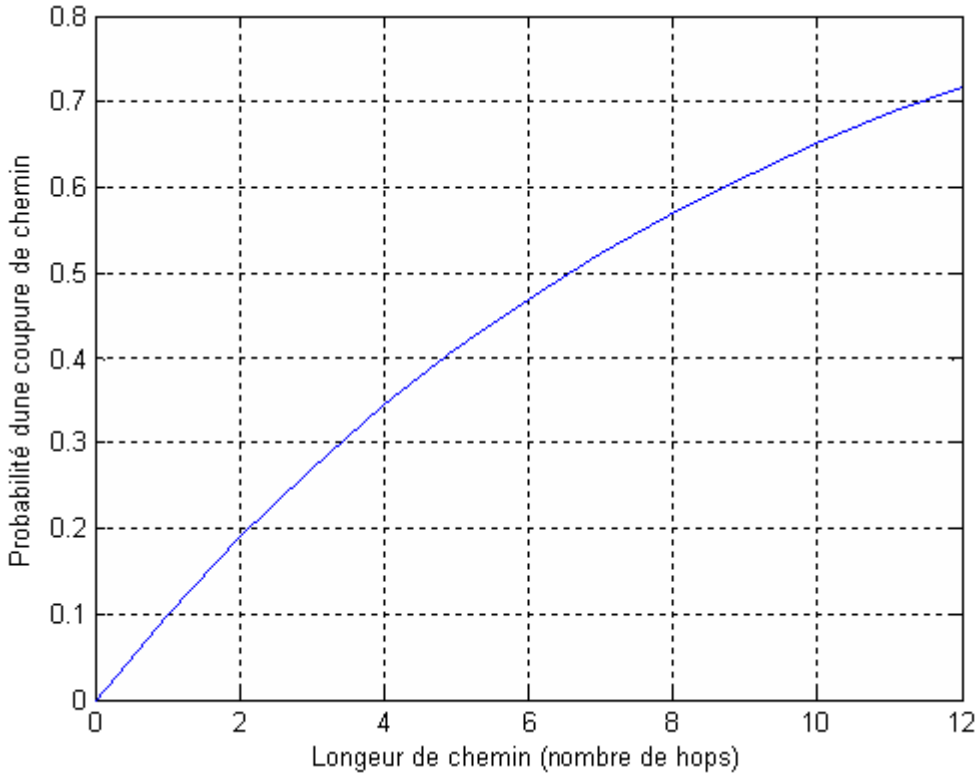


Figure 2.1 : Probabilité de rupture d'un chemin selon le nombre de saut.

4. Recalcule du chemin entre DSR et AODV :

Sur NS2 "Network simulator" voir annexe, On faire une comparaison entre le protocole AODV et le protocole DSR, le but de cette simulation est de voir le temps écoulé pour récupère une route défaillante entre une source et un destinataire, pour cela on défini trois routes différentes, puis à un temps donné, on fait quitter des nœuds appartient au chemin entre la source et le destinataire, donc la source doit retrouver une nouvelle route valide vers le destinataire, les résultat de la simulation sont montré dans la figure ci-dessus

Type de Trafic	FTP
Nombre de nœuds	14
Transport	TCP
Protocole de Routage	AODV, DSR
Temps de la simulation	50s

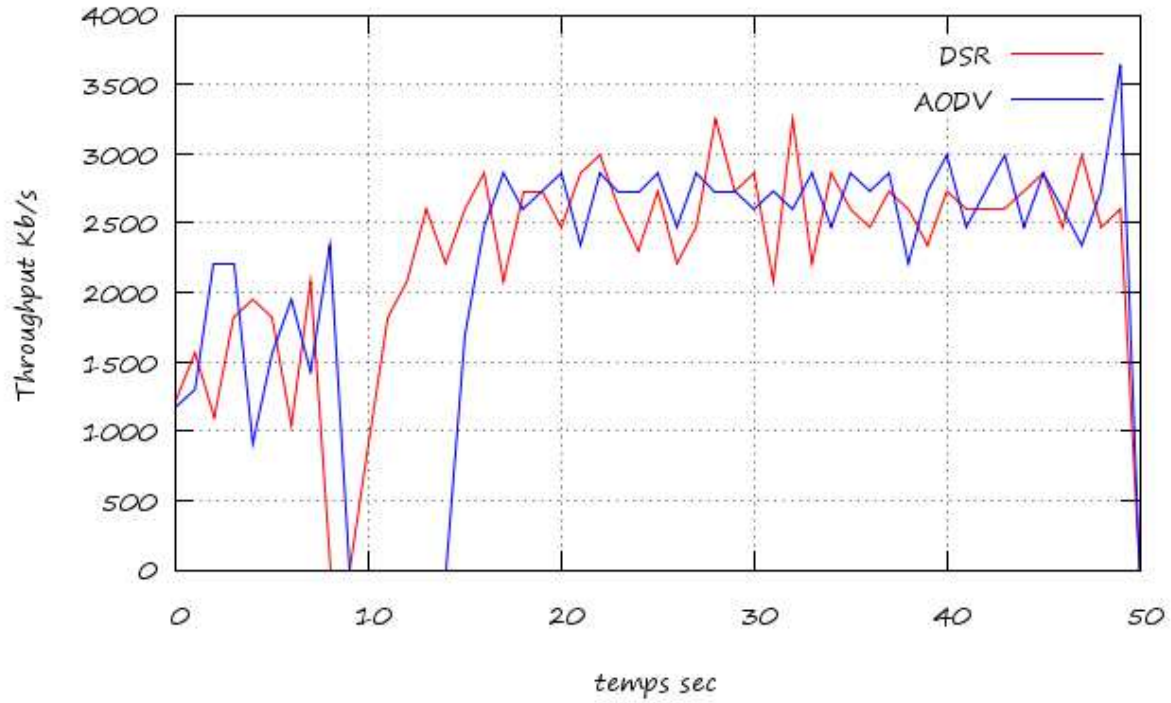


Figure 2.2 : Récupération du transfert cas DSR et AODV

D'après les résultats de la simulation, le protocole DSR apparaissent meilleurs que le protocole AODV concerne la récupération du transfert des données (1.5s pour DSR vs 4s pour AODV), cela revient comme on a déjà vu dans le chapitre précèdent dans le délai d'établissement du chemin, aussi AODV supporte seulement les liens symétrique, un lien asymétrique considère comme invalide, cette propriété influe fortement sur le temps de la reconstruction du chemin.

5. Les protocoles de routage multi-chemins

Le routage à chemins multiples consiste à trouver plusieurs chemins entre une source et une destination, ces chemins sont exploités selon différente manière [3] afin de compenser la mobilité des nœuds et la nature imprévisible des réseaux ad hoc. Pour cela La conception des protocoles de routage multi-chemins doit repose sur plusieurs contraintes citons :

Comment découvrir des chemins multiples

La plupart des protocoles multichemin sont de nature réactif, afin de prendre en charge les contraintes du multichemin, les mécanismes de découverte de routes basés sur DSR ou AODV doivent être modifiés pour découvrir un maximum de routes entre une source et une destination donnée, la présence des ressources (liens ou nœuds) partagées entre ces route dégradent les performance du protocole, donc trois type de routes peuvent être mise en place:

- **Routes disjointes en nœud** : les nœuds des différents chemins ne doivent pas être communs, un nœud intermédiaire appartient à un seul chemin à la fois pour un couple source/destinataire

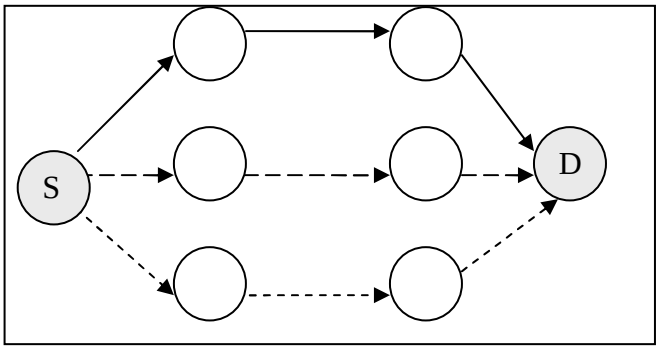


Figure 2.3 : Chemins disjoints en noeuds

Les chemins entre S et D, ne contiennent ni un lien, ni un nœud en commun.

- **Routes disjointes en lien** : les liens de différents chemins ne doivent pas être communs, mais peuvent avoir des nœuds en commun.

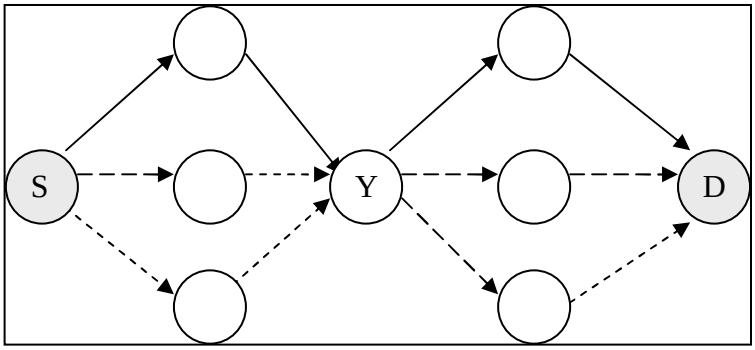


Figure 2.4 : Chemins disjoints en lien

Les routes disjointes en lien : chemins entre S et D ont un nœud (Y) en commun

- **Routes non disjointes** : ils existent soit des nœuds soit des liens en commun.

En termes de robustesse des chemins et de tolérance aux pannes, les algorithmes qui se basent sur les routes disjointes en nœud versus en lien offrent un certain avantage par apport à celles non disjointes. Quand on utilise des routes non disjointes, l'échec d'un lien ou la panne d'un nœud peut causer la rupture de plusieurs routes, cependant pour les routes qui sont disjointes en lien l'échec d'un lien peut seulement provoquer la rupture de la route dans laquelle il est inclus, mais la panne d'un nœud peut provoquer la rupture de plusieurs routes. Les routes disjointes en nœud offrent le plus haut degré de tolérance aux pannes car la défaillance d'un nœud ou la rupture d'un lien peut causer la rupture d'un chemin au plus.

En termes de délai de découverte des chemins et de complexité d'implémentation. Les routes non disjointes sont plus faciles, parce qu'il n'y a aucune restriction sur la construction des chemins. Par conséquent la découverte des routes disjointes en nœuds est moins abondante et dur à trouver. Dans un réseau dense, il peut exister un nombre limité de chemins entre deux nœuds arbitraires, particulièrement quand la distance entre les nœuds, augmente. [8]

Comment choisir un chemin :

Une fois que plusieurs chemins sont découverts, la question qui se pose est combien de chemins seront réellement utilisés ? Si peu de routes sont utilisées, les performances du protocole de routage multichemin peuvent être comparables à celles du plus cours chemin dans le cas de routage *unipath*. Cependant si tous les chemins sont utilisés il y a de forte chance d'utiliser de longs chemins ce qui va influencer négativement sur les performances du routage multichemin [9].

Plusieurs protocoles de routage multichemin ont été proposés. Ces protocoles peuvent être classés selon l'objectif sur lequel ils ont été conçus : la fiabilité, la robustesse des chemins, la rapidité de recouvrement, répartition de la charge et la conservation énergie, mais il est rarement de trouver un protocole qui satisfait toutes ces contraintes en ensemble. Un protocole peut assurer la fiabilité de la connexion par la découverte de plusieurs routes à la fois, toute en gardant le même trafic pour construire ces routes.

5.1 Split Multi-path Routing protocol (SMR)

SMR a été présenté dans [7], l'objectif principal de celui-ci consiste à construire un nombre maximum de chemins disjoints entre une source et une destination, où la charge du trafic est partagée sur les différents liens tout en évitant la congestion des nœuds, ce qui permet une utilisation efficace des ressources disponibles du réseau.

La construction des routes dans **SRM** est basée sur le cycle *Request/Replay*. Quand un nœud source veut transmettre un message, elle diffuse un paquet requête de type RREQ à travers le réseau, lorsque le destinataire reçoit ce paquet par des chemins différents, il choisit parmi eux les chemins disjoints, et répond par un paquet de type RREP qui sera envoyé vers la source à travers ces chemins choisis.

Le mécanisme de base de découverte de routes dans **SMR** est inspiré de celui utilisé par le protocole **DSR**, avec la particularité qu'un nœud intermédiaire n'est pas autorisé à envoyer un paquet RREP si la route est déjà identifié dans sa *table cache* vers le même destinataire (cas du : **DSR** et **AODV**) cette idée facilite au destinataire de calculer des chemins disjoints. Afin de construit le maximum des chemins disjoints, une modification introduite sur le traitement des paquets dupliqués, si un nœud reçoit des RREQ dupliqués il ne l'écarte pas tous (cas **DSR**) seulement les RREQ qui arrivent de routes différentes et qui ont un nombre de sauts (*hop_count*) qui n'est pas plus grand que celui du premier RREQ reçu seront rediffusés.

La faiblesse de cette approche réside dans le temps de validité des routes alternatives, si les nœuds du réseau déplacent avec une vitesse assez élevé, les chemins enregistrés dans la table cache du nœud source devient invalides, sans le savoir préalable de la source, s'il y a une rupture dans la route primaire, la source va tester les routes alternatives l'une après l'autre et le résultat aucune route reste n'est valide, implicitement la source doit relancer un nouveau processus de découverte de la route.

Suggestion :

Pour améliorer les performances de ce protocole, nous proposons l'ajout d'une fonction au niveau de la source, cette fonction permet à la source de contrôler l'état de chaque chemin alternatif, la source émet périodiquement un message vers le destinataire nous l'appelons "persister_la_route", sur tous les chemins alternatifs ou choisir un sous ensemble. Avec cette méthode si le destinataire est inaccessible via le chemin primaire la source sait bien l'état de chaque route (valide ou invalide), cette proposition est coûteuse en terme de surcharge, mais elle est plus performante si les nœuds du réseau déplacent avec une vitesse assez importante. Cette fonction est montrée dans l'algorithme suivant :

```
Etat (chemin_alternatif i) := Valide
Pour i=1 à nombre_chemin_alternatif faire
    Si État (chemin_alternatif i) = Valide alors
        Envoyer (test_chemin i)
    Finsi

    /*attendre l'arrivé d'un acquittement*/

    Si NON-ACK (test_chemin i) alors      /* absence d'un acquittement*/
        État (chemin_alternatif i) : = Invalide
    Finsi

Fin pour
```

5.2 Protocole AOMDV

Pour améliorer les performances du protocole **AODV**, plusieurs versions de routage multichemin basé sur AODV ont été proposées. L'un de ces approches nommée **AOMDV** "Ad hoc On-demand Multipath Distance Vector Routing" qui a été proposé dans [8]. AOMDV permet de créer des routes multiples disjointes en liens ou en nœuds et sans boucle de routage, dans l'ordre d'évite la création de ces boucles les auteurs appliquent le même principe d'AODV, qui consiste à n'accepter une nouvelle requête que si : le nombre de sauts est inférieur ou que le numéro de séquence est supérieur.

Dans AOMDV les routes multiples sont formées pendant la phase de découverte de la route, pour cela les auteurs définssent un nouveau concept, qui est le "*advertised_hopcount*" remplaçant le paramètre "*hopcoun*t" du protocole AODV voir figure 2.3, ce paramètre représente le maximum "hopcount" des routes disponible d'un *I* nœud vers la destination *D*. Pendant la phase de découverte de la route si un nœud reçoit des copies d'une même requête RREQ, il ne rejeté pas immédiatement (cas de AODV) mais il l'examine selon le paramètre "*advertised_hopcount"* notons aussi que chaque RREQ arrive d'un voisin définie un chemin disjoint en nœuds ceci parce que les nœuds intermédiaires ne diffuse pas les RREQs dupliqués donc deux requêtes arrivent à un nœud n'a pas pu avoir traversé les mêmes nœuds. Dans une tentative d'obtenir des chemins disjoins en lien, le destinataire répond avec un RREP seul aux requêtes arrivant depuis des voisins distincts, les RREPs chacune prend un chemin inverse, les trajets de ces RREP peut intersecté dans des nœuds intermédiaires mais chacune prend un chemin différent vers la source ceci également suffisant que les chemins seront disjoint en lien. Pour la maintenance de la route AOMDV ne lance pas un nouveau

processus de la découverte seulement si aucune des routes précédemment établies n'est valide.

destination
numéro de séquence
advertised_hopcount
Liste_de_route {(nexthop1,hopcount1), (nexthop2, hopcount2), …}
expiration_timeout

(a) AOMDV

destination
numéro de séquence
hopcount
nexthop
expiration_timeout

(b) AODV

Figure 2.4 Structure des tables de routage dans AODV et AOMDV.

La figure montre les différents changements dans AOMDV, une liste appelée " Liste_de_ route" remplace le prochain saut "hopcount" de AODV, cette liste définie pour chaque prochain saut "nexthop$_i$" le nombre de saut "hopcountj" nécessaire pour atteindre la destination en passant par ce nœud

Afin de garantir les performances entre le protocole AOMDV et sa version unipath AODV on faire une simulation. Dans cette simulation on faire quitter un nœud qui appartient au chemin de transfert .La figure ci-dessus montre les résultats de cette simulation :

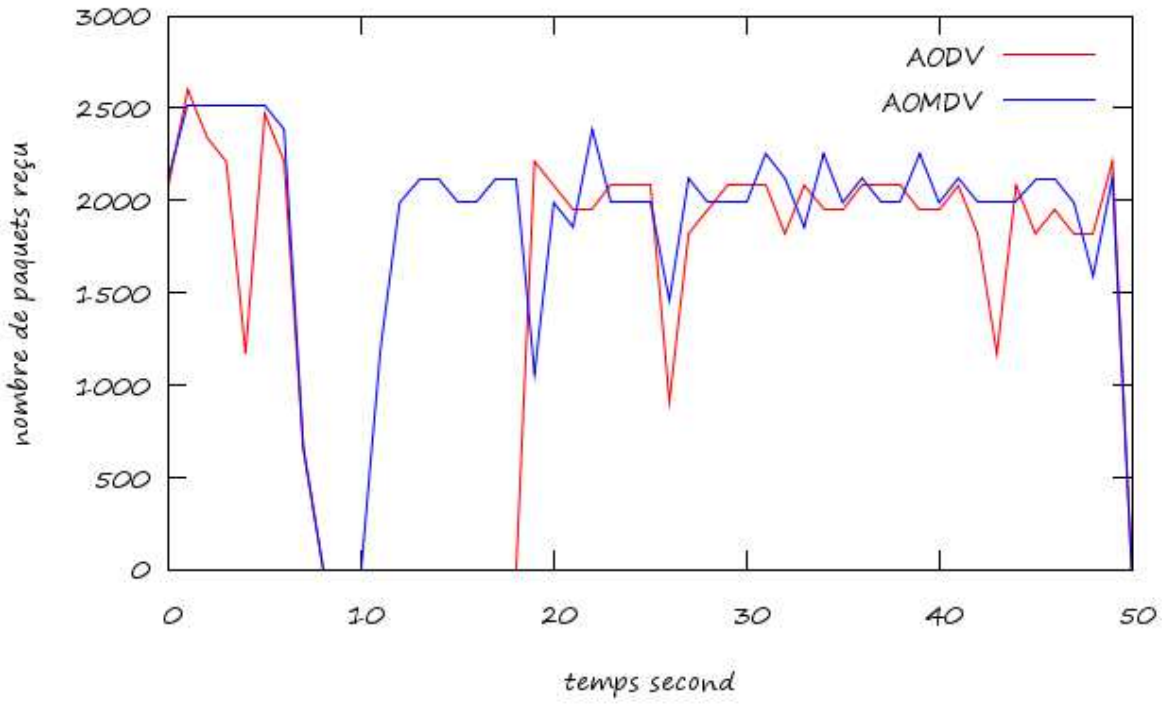
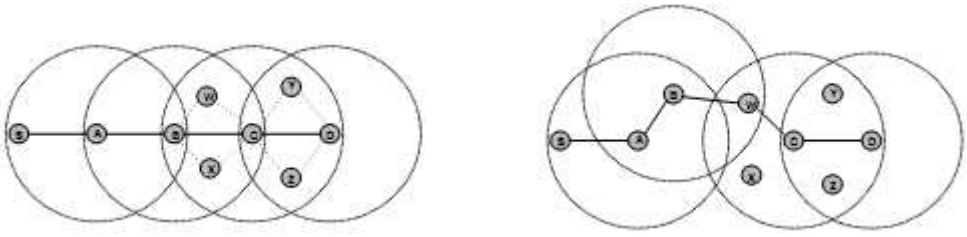


Figure 2.5 : récupération de la route cas des protocoles AODV, AOMDV

La figure montre le grand avantage du protocole multichemin AOMDV comparant au protocole AODV en terme de la rapidité de reprendre le transfert des données. Le AODV doit relance un nouveau processus de découverte de la route afin de trouver une route valide, au contraire le protocole AOMDV utilise seulement sa base local, qui incluse de nombreux

chemins définis au préalable dans le processus de découverte de la route, un autre avantage du protocole AOMDV concerne le nombre total des données reçus par le destinataire.

Une autre approche multichemin basé sur le protocole AODV, nommée BR-AODV a été présentée dans [5], la construction de ces routes est effectué pendant la phase de réponse, en exploitant les propriétés de la diffusion dans les réseaux sans fil, quand un nœud *X* intermédiaire envoie une réponse de la route RREP vers un nœud *Y* pour construire un chemin (primaire), les autres nœuds qui situent à porté du nœud X vont aussi recevoir ce paquet donc il enregistrent ce nœud X comme étant *next-hop* vers le destinataire dans une table Alternatif-Route et l'utilise en cas de rupture de lien entre les nœuds X et Y. La figure suivante montre le recouvrement de la route s'il y a une rupture d'un lien



Chemin primaire entre S et D Recouvrement de la route

Figure 2.6 : le chemin primaire BR-AODV

- Avantages :
  - Cette approche n'ajoute aucun trafic de contrôle supplémentaire.
  - Aucune modification dans la structure ou dans le processus de découverte de la route implémenté dans le protocole AODV
- Inconvénient :
  - Cette approche traite uniquement le problème de mobilité d'un nœud appartient au chemin primaire, elle néglige le cas où un nœud tombe en panne ou quitte le réseau.

5.3 Protocole Redundant Source Routing (RSR):

Ce protocole a été présenté dans [9], l'algorithme utilise des routes disjointes en nœuds. L'idée de base derrière ce protocole est avant qu'un transfert a eu lieu, le message est subdivisé en sous messages, puis chacun sera envoyé sur un chemin distinct, le but de cette approche est d'augmenter la fiabilité de routage. S'il ya un échec sur un chemin la chance de transfert avec succès sur d'autres chemins reste. Il y a donc une dispersion de routage.

Un message est divisé en sous messages, avec un nombre de sous messages inférieur au nombre des chemins découverts. Des messages supplémentaires sont construits comme une combinaison linéaire avec les bits du message original. Ceci permet au destinataire la reconstruction du message initial même si les sous messages n'ont pas été tous reçu.

RSR est un protocole de routage orienté source, le destinataire est lui le responsable de la construction des chemins disjoints. Le premier chemin construit étant $Path_1$ qui détient le nombre de saut h_{min}, les autres chemins ont un nombre de saut $h_{min}+1$, $h_{min}+2$,……, h_{max} et qui sont disjointes avec $Path_1$, RSR choisit deux chemins, l'un est choisi comme primaire qui est le plus court chemin, l'autre choisi comme secondaire, le chemin alternatif choisit selon un mode round-robin, deux paquets identiques sont envoyés sur les deux chemins, une copie est envoyée sur le chemin primaire, l'autre copie est transmise sur le chemin alternatif. La

duplication se réalise par le mécanisme suivant : au niveau de la couche réseau RSR ajoute un agent, nommé PDA (*Packet Duplication Agent*) son rôle est d'assurer la duplication des paquets avant de les transmettre, quand un paquet passe de la couche supérieure à la couche réseau, il est intercepté par le PDA, puis un filtrage est effectué sur ces paquets que ce soit qu'il s'agit d'un paquet de données ou un paquet de contrôle (ACK, RREQ ou RREP). Seulement les paquets de type TCP ou UDP seront dupliqués. Au niveau récepteur la couche réseau a aussi un autre agent PFA (*Packet Filter Agent*), dont son rôle est d'assurer le filtrage et la destruction les paquets dupliqués.

Comparativement à DSR, RSR est plus fiable, car il diminue le nombre de paquets perdus et offre une rapidité dans la réparation des routes interrompues, l'inconvénient cette technique réside dans le fait qu'elle est inadaptée pour les protocoles qui ne gèrent pas des numéros de séquence au niveau de la couche transport (par exemple : UDP). La maximisation des routes alternatives présente aussi un souci, la source doit être informée de la rupture de chaque route, en plus, plusieurs copies identiques qui traversent deux chemins différent, arrivent au récepteur intacts ce qui est considéré comme une utilisation inefficace des ressources réseau (énergie, bande passante). Ainsi l'ajout des agents de duplication et de filtrage augmente le délai de traitement inter-couches en émission et en réception.

5.4 Multi-chemins pour le transport de la vidéo

Le transport de la vidéo avec ses contraintes et sa QoS (bande passante, délai, temps réel, etc.) à travers les réseaux ad hoc pose un grand défi. Des recherches sont en cours pour que les réseaux ad hoc prennent en charge ce type de service, l'idée est d'utiliser un routage multichemin qui présente une solution efficace permettant de surmonter les contraintes qui caractérisent ce type d'application.

Une approche qui a été présentée dans [10], elle utilise un routage multichemin pour le transport de la vidéo à travers les réseaux ad hoc, le but de cette approche est de réduire le nombre de paquets perdus, qui dû au changement de la topologie du réseau. La construction des routes dans RMPSR (Robust Multipath Source Routing Protocol)) repose sur un facteur de corrélation deux routes (rapport entre le nombre des nœuds partagés entre deux routes et le nombre de nœuds dans le plus cours chemin), deux routes sont *presque disjointes* si leur facteur de corrélation est petit qu'une valeur donnée [10]

RMPSR définit les concepts suivants :

- *Set-route* : constitué d'un *chemin primaire* et de plusieurs *chemins alternatifs*,
- chemin primaire : connecte un nœud source et un destinataire,
- chemin alternatif : connecte un nœud intermédiaire et un destinataire,
- Deux set-routes sont presque disjointes si ses routes primaires sont presque disjointes.

L'idée de base de RMPSR est de créer le plus possible des routes presque disjointes, la découverte des routes est inspiré de DSR c'est-à-dire que le destinataire a la responsabilité de construire ces routes. Quand le destinataire reçoit plusieurs copies RREQ d'une même source, elle collecte dans une fenêtre temporelle, ensuite il construit des routes presque-disjointes, et enfin il retourne le chemin primaire vers la source et les chemins alternatifs vers les nœuds intermédiaires.

RMPSR utilise un schéma d'allocation qui distribue les paquets sur deux routes primaires différentes appartenant au même set-route, si la source reçoit un message RERR (*Route Error*) indiquant la rupture de la route, le nœud source commute le transfert vers la deuxième route. Les auteurs de RMPSR proposent une approche dédiée pour les applications vidéo afin de surmonter le problème des liens rompus. Pendant le transfert des paquets si un lien est interrompu, les paquets qui sont transportés sur ce chemin seront commutés systématiquement vers des chemins alternatifs qui appartiennent au même set-route, puis le nœud intermédiaire envoie un message RERR vers la source lui indiquant la rupture d'un lien, la source retire immédiatement ce chemin défectueux puis commute le transfert vers d'autres chemins primaires appartenant à un autre set-route.

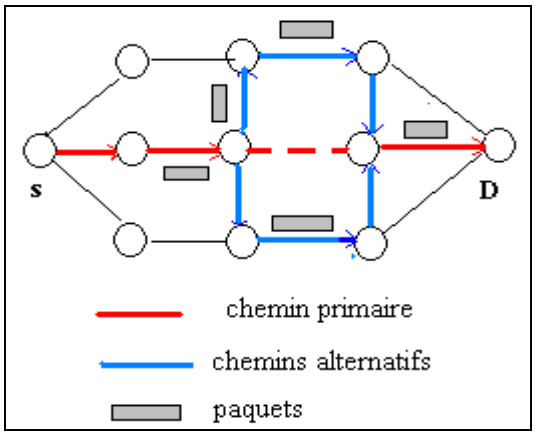


Figure 2.7 : Traitement du problème de rupture des liens dans RMPSR

Cette approche à l'avantage de diminuer le nombre des paquets perdus et augmente le rapport de livraison des paquets, sans avoir recours à la retransmission, et assez de trafic de contrôle pour la maintenance des routes interrompu

6. Synthèse sur les protocoles existants

Plusieurs algorithmes de routage multichemin ont été proposés, et chaque protocole possède ses forces et ses faiblesses, mais rarement où on trouve un protocole qui combine plusieurs paramètres (délai, congestion énergie, etc.), le tableau suivant résume ces algorithmes tout en mentionnant le but principal de chaque algorithme et l'approche sur laquelle s'articule.

But principale	protocole	approche
Réduire le délai	Frsesnel Zone Routing	Distribue le trafic sur différente zone
Améliorer la fiabilité	Caching and Multipath Routing	Utilise une diversité de codage pour réduire le taux erreur
Minimiser la charge	Split Multipath Routing SMR	Seul le nœud destinataire qui envoie un RREP
Efficacité d'énergie	Multipath On-Demand Routing	Conserve l'énergie par réduction du trafic non nécessaire

7. Conclusion

Les protocoles de routage dans les réseaux ad hoc sont de type réactif ou proactif, cependant ces protocoles sont de type mono chemin c'est-à-dire un seul chemin défini à la fois entre une

source et un destinataire donnée, la rupture d'un lien entre nœuds intermédiaires implique la rupture total du chemin, de ce fait la récupération du transfert des données, nécessite le lancement d'un nouveau processus de découverte de la route.

Les protocoles de routage multichemin, peuvent résoudre ce problème puisqu'ils assurent une multitudes de routes entre les nœuds communicant, cela se faire pendant la phase de découverte de la route sans la génération d'un trafic supplémentaire sur le réseau, aussi ces protocoles améliorent beaucoup les performances des réseaux ad hoc soit en terme de fiabilité ou robustesse face aux différentes ruptures des routes, ainsi le multichemin résoudre le problème de la congestion des nœuds intermédiaire par une répartition équitable de la charge sur les différent noeuds du réseau toute en évitant la compensation du trafic sur un chemin unique et explicitement le multichemin maximiser la vie total du réseau ad hoc .

Malgré tous les avantages du routage multi chemins (minimisation de re-calcule des chemins, disponibilité des routes, ….) un problème potentiel de cette solution réside dans le niveau transport de la pile des protocoles TCP/IP, qui est responsable, à la délivrance et la assemblage / dé-assemblage des paquets, l'utilisation de plusieurs routes simultanément complique la gestion des temporisateurs manipulé par TC , et la taille des différent fenêtres manipulé par les protocoles de la couche transport cela revient que chaque chemins a ces propre paramètres (temporisateurs, fenêtres..), ainsi l'envoi des paquet sur différent chemins provoque l'arrive des paquets dans le désordre Out-Of-Order, ou hors séquence. La problématique de la couche transport on la traite dans le chapitre suivant

Référence:

[1] Y. Ganjali, A. Keshavarzian "*Load Balancing in AdHoc Networks: Single-path Routing vs. Multi-path Routing*" journal IEEE 2004

[2] G. Parissidis, V. Lenders, M. May, and B. Plattener. "Multi-path Routing Protocols in Wireless Mobile Ad Hoc Networks: A Quantitative Comparison." Proceedings of 6th International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking NEW2AN 2006, St.Petersburg, Russia.

[3] M.Tarik , K E. Tepe , S. Adibi "*Survey of multipath routing protocols for mobile ad hoc networks*" journal of network and computer application 32 (2009)

[4] S. Charoenpanyasak "Optimisation inter-couches du protocole SCTP en réseaux ad hoc" thèse doctorat juin 2008

[5] S. Lee, M. Gerla "*AODV-BR: Backup Routing in Ad hoc Networks*", proceeding of the IEEE Wireless Communication and Networking Conference (WCNC), September 2000

[6] X. Zhu, B. Girod "*A Distributed Algorithm for Congestion-MinimizedMulti-Path Routing over Ad hoc Network*s"

[7] Lee, S., Gerla, M.:"*Split multipath routing with maximally disjoint paths in ad-Hoc networks*" .Proceedings of the IEEE ICC (2001) 3201–3205

[8] M.K.Marina , S.Das, "On-Demand multipath distance vector routing in ad hoc networks" in: Proceedings of the 9th IEEE International Conference on Network Protocol 2001

[9] Wang L, Jang S, LeeT-Y "Redundant source routing for real-time services in ad hoc Networks" In: Proceedings of IEEE international conference on mobile ad hoc and sensor systems conference, Washington, DC, November, 2005

[10] Wei W,Zakhor A. "Robust multipath source routing protocol (RMPSR) for video communication over wireless ad hoc networks". In IEEE international Conference on multimedia and expo ICME 2004

[11] Mao S, Lin S, Wang Y, Panwar SS, LiY. "Multipath video transport over ad hoc networks" IEEE Wireless Communication August 2005

[12] W.Lou, W.liu, Y.Fang "spread: improving network security by multipath Routing" Journal IEEE 2003

Chapitre 3 :

Auto configuration d'adresses IP pour les réseaux ad hoc

1. Introduction

Un réseau mobile ad hoc est un réseau auto-organisé et auto-configuré où chaque nœud fonctionne comme un nœud terminal et un relais sans fil, cette forme du réseau est crée sans l'existence préalable d'une infrastructure fixe ou d'une entité centrale, parmi les majeurs enjeux dans les réseaux ad hoc, l'auto-Configuration qui signifie l'acquisition systématique d'une adresse IP correspondante pour chaque nœud du réseau ad hoc sans l'aide d'un administrateur système.

Tous les protocoles de routage décrits précédemment assument que les nœuds du réseau sont identifiés entre eux, mais la réalité est que : avant de participer dans toute communication, les nœuds du réseau ont besoins de s'identifiés exclusivement et mutuellement entre eux d'où l'identificateur de chaque nœud est son adresse IP, cette adresse doit vérifier l'unicité pendant l'existence du nœud dans le réseau ad hoc.

L'auto configuration dans les réseaux filaires s'articule sur la présence d'une entité centrale tel un serveur DHCP "Dynamic Host Control Protocol" [1], qui assigne des adresses IP aux différents nœuds du réseau. Cette solution ne peut être implémentée dans les réseaux MANET, à cause de la mobilité des nœuds, ainsi un serveur DHCP peut être inaccessible durant un temps, ce qui empêche la progression du réseau.

Une adresse IP est un nom logique attribué à un interface physique, dans la version IPv6 une adresse IP est définie sur 128 bits au lieu de 32 bits dans IPv4, ce changement dans la taille d'adresse est due des limitations existe dans le système d'adressage IPv4 [10], en générale le mécanisme d'auto configuration d'adresses dans IPv6 d'adressage est plus compliqué, mais l'avantage du IPv6 est que les adresses peuvent être configurées automatiquement avec ou sans la présence d'un serveur DHCP, ce qui simplifie beaucoup la tache de l'administrateur.

2. Problème d'adressage dans les réseaux ad hoc :

L'auto configuration dans IPv6 signifie qu'un nœud acquis une adresse à partir d'un identificateur local (interface réseau), cette adresse est constituée de deux parties, l'une c'est l'adresse MAC codé sur 64 bits, l'autre partie c'est le préfixe du réseau codé sur 64 bits, Pour les anciennes interfaces réseaux IEEE leurs adresse MAC est codées sur 48 bits ce qui nécessite un mécanisme pour étendre vers 64 bits (figure3.1).

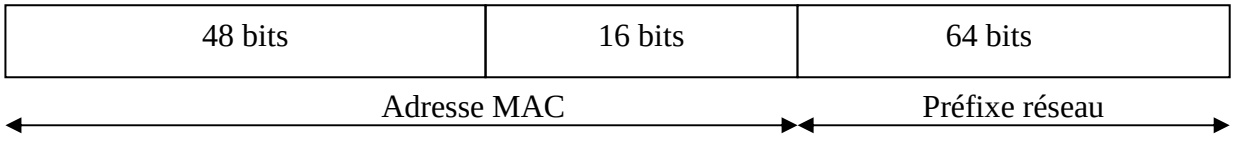


Figure 3.1 format générale d'une adresse IPv6

Cependant un adressage basé sur un identificateur hardware pose certaines limites à cause de:

1. problème d'unicité des adresses MAC [6], quelques produits n'ont pas enregistrés au sein de l'organisme IEEE, ainsi il est possible de changer l'adresse MAC par une reprogrammation du EEPROM ou par modification d'adresse MAC dans la mémoire du système [4]

2. une mal fabrication des interfaces peut engendre des adresses MAC dupliquées [8]
3. hétérogénéité des nœuds qui forment le réseau ad hoc, quelques nœuds n'utilisent pas 48 bits comme une adresse MAC, ils utilisent d'autres tel le code IMEI

Donc, les nœuds doit utilise un autre processus pour acquérir une adresse IP, pour cela plusieurs approches sont proposées.

3. Requis d'un protocole d'attribution d'adresse IP :

Un protocole d'assignement d'adresses IP doit satisfaire les contraintes suivantes :

- Manque de conflit dans le processus d'affectation des adresses IP, c'est à dire dans un instant donné il existe qu'un seul nœud possèdent une adresses IP unique
- Une adresse IP est affecté pour une durée où le nœud existe dans le réseau, dés que le nœud quitte le réseau son adresse IP doit être disponible pour l'utilisation par d'autre nœud
- Le protocole doit prise en charge le cas où il y a un partitionnement ou un fusion. quand il y a une fusion entre deux réseaux ou plus, une possibilité que plusieurs nœuds ont la même adresse IP .alors la duplication d'adresses doit être détecté immédiatement
- Pour un aspect de sécurité, un tel protocole doit assurer que sauf les nœuds autorisés doit bénéficie d'une configuration et d'une permission d'accès au réseau

Divers arguments évaluent les performances d'un tel protocole d'assignement d'adresse IP, la complexité de l'algorithme, le nombre total de communication avant la validation d'adresse et le délai pour acquérir une adresse IP

4. Partitionnement et fusion des réseaux ad hoc :

La division d'un réseau MANET en plusieurs réseaux indépendants connus sous le nom partitionnement, cette division peut être de deux types, volontaire ou involontaire, si les nœuds quittent le réseau après informes ses voisins cela c'est volontaire, l'autre cas c'est quand les nœuds quittent le réseau d'une façon involontaire sans aucune négociation avec ces voisins, cette dernière peut engendre une perte de quelques adresses IP. ce qui nécessite quelques mécanismes de la détecte

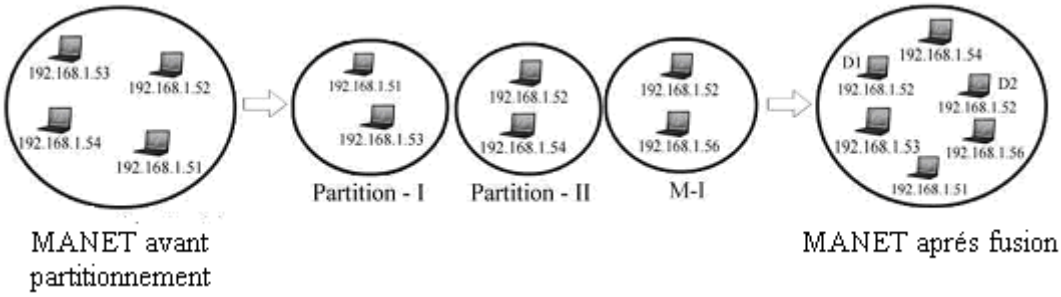


Figure 3.2: Partitionnement & fusion des MANETs

La perte des adresse IP, avant le partitionnement un seul réseau existe avec sa propre plage d'adresses de 192.168.1.51/24 à 192.168.1.54/24 après le partitionnement il divise en deux réseau Ad-hoc indépendants chacun constitué à des adresses hérité du réseau MANET originale .les adresses dans la partition ***I*** ne peuvent assigné pour des nouveaux nœuds veulent entrer dans la partition ***II*** et vise versa. Ce qui diminue le nombre d'adresses IP qu'on peut l'allouer

La combinaison de deux ou plusieurs réseaux ad hoc dans un seul réseau est appelé fusion [2], cet événement apparu lorsque plusieurs réseaux indépendants se réunir afin de former un seul réseau, cette fusion peut engendre un conflit les différentes d'adresse IP existantes dans chaque groupe. La figure 3.2 montre cette situation, les partitions I, partition II &M-I sont des réseaux de type ad hoc indépendants et chacun utilisent ses propre plage d'adresses IP, si ces réseaux ont réunis, quelque nœuds peuvent avoir la même adresse IP (cas D1& D2), pour surmonter ce problème un processus DAD "Duplicate Address Detection" est indispensable.

5. Le processus de Détection des adresses Dupliquées (DAD) :

L'auto configuration d'un nœud IPv6, signifie qu'un nœud génère et acquis une adresse IP, pour assurer l'unicité de cette adresse dans le réseau, chaque nœud génère un message vers tous les nœuds du réseau, si l'un des nœuds utilise cette adresse il doit répondre à cette requête. Si aucune réponse au bout d'un temps, l'adresse est assume comme unique et le nœud peut l'utilise pendant son existence dans le réseau. Ce processus est appelé DAD (Duplicate Address Detection)

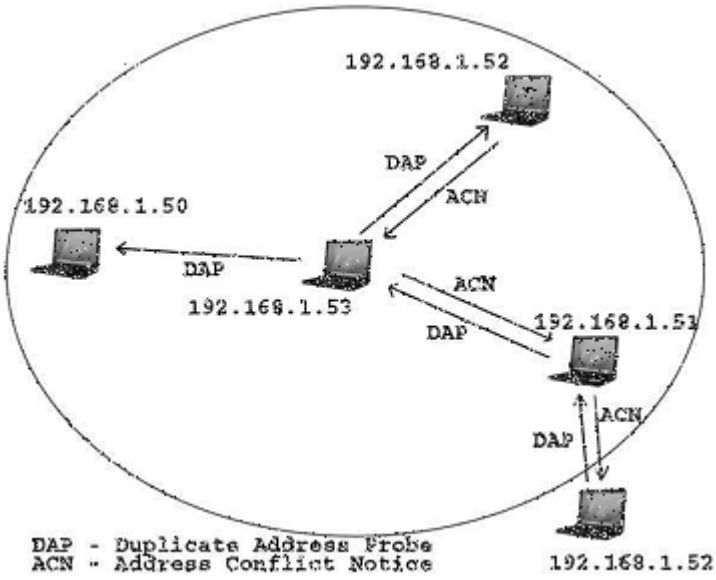


Figure 3.3 : Mécanisme de Détection adresses Dupliquées

Le protocole DAD est nécessaire quand un nouveau nœud veut joindre le réseau, ou lorsque plusieurs réseaux viennent d'être fusionnés dans un seul réseau. Ici on note que tous les nœuds possédant une adresse IP valide doivent être participés dans ce processus, ceci permet de protéger leurs adresses contre une utilisation accidentelle par un nouveau nœud.

La vérification des adresses IP dupliquées est basée sur le mécanisme "question / réponse", un nouveau nœud choisit une adresse IP, puis envoie un message DAP "Duplicate Address Probe" contenant cette adresse, ce nœud attendre l'arrivé d'un message ACN "Address Conflict Notice", qui annonce que cette adresse est déjà utilisée, si au bout d'un temps 'T' ou après 'N' nombre de tentative le noeud ne reçoit aucun message ACN, le noeud assume que l'adresse est inutilisable, et peut l'utiliser ce processus est illustré au figure 3.3

6. Schémas d'allocation d'adresses IP pour les MANET :

La configuration d'adresses pour les nœuds d'un réseau ad hoc peut être réalisée soit par le nœud lui-même à partir des paramètres internes, soit sous la responsabilité d'autres nœuds qui font déjà partie du réseau. Plusieurs travaux sur ce sujet proposent des solutions pour résoudre ce problème, nous pouvons distinguer différentes catégories [8] : la configuration sans détection de conflit et la configuration avec détection de conflits :

6.1 Schémas avec état (statfull) :

Dans cette catégorie les nœuds qui font partis du réseau assument la responsabilité de configurer des nouveaux nœuds qui désirent rejoindre le réseau, on les fourni une adresse IP valide afin de participer aux communications dans le réseau ad hoc, plusieurs protocoles sont proposés, on limite notre étude aux deux approche :

6.1.1 MANETconf :

Proposée dans [4], l'unicité d'adresse est assurée par le biais de deux tables T-pending pour les adresses candidats et T-allocated pour les adresses allouées. Le schéma d'attribution d'adresse démarche de la manière suivante : lorsque un nouveau nœud X désire de joindre le réseau ad hoc, diffuse un message "Neighbors_Query" vers ses voisins qui doit répondent avec "Neighbor Reply", si au bout d'un temps T pas de réponse le nœud X affirme qu'il est le premier nœud dans le réseau et assigner une adresse IP à son interface. S'il y a des réponses le nœud X choisi arbitrairement un des voisins Y comme un **initiateur**, et l'envoie un message "Requester _Request" afin de réclame une adresse IP. Le nœud Y choisi une adresse ADDx et l'ajout dans sa table T-pending. Puis diffuse un message contient cette adresse vers tous les nœuds du réseau. Chaque nœud dans le réseau vérifie dans ses tables l'existence de cette adresse et renvoyer une réponse vers le nœud Y .si toutes les réponse sont positifs le nœud Y affirme que cette adresse n'est plus utilisé, il déplace cet adresse vers T-allocated et assigné au nœud X cette adresse sans aucun conflit avec d'autres nœuds et diffuse vers tout les nœuds du réseau un message indique que cet adresse est assigne au nœud X , chaque nœud déplace cette adresse de T-pending vers T-allocated .cette adresse devient valide et le nœud X peut commencer ses communication dans le réseau . Dans l'autre cas le nœud Y répète le processus avec une autre adresse.

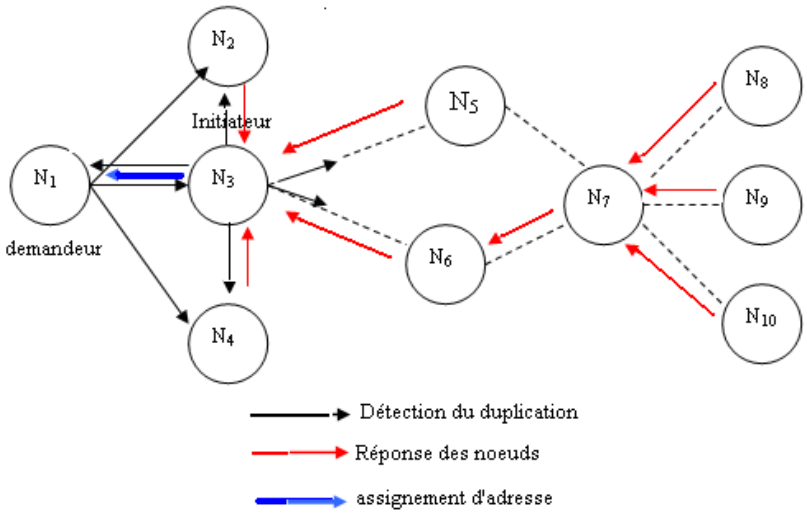


Figure 3.4 : assignement d'adresse dans MNAETconf

(1) le nœud N_1 non configuré cherche un voisin comme un initiateur
(2) le nœud N_3 choisis arbitrairement une adresse, puis diffuse un message vers le réseau entier, si cette adresse est occupée.
(3) Les nœuds du réseau, répondent, avec un message.
(4) Selon la réponse N_3 affecte cette adresse au nœud N_1, ou redémarre le processus avec d'autre adresse.

6.1.2 Le système "Buddy system" :

Cette approche basé sur une division binaire d'une plage d'adresse IP, les nœuds du réseau jouent collectivement le rôle d'un serveur DHCP, où chaque nœud dans le réseau avait capable de configurer un nouveau nœud désire de rejoindre le réseau, on lui offre un adresse IP valide, les nœuds du réseau ont besoin un certain niveau de synchronisation afin d'actualisent leurs informations d'adressage sur le réseau.

Dans un système buddy [2] chaque nœud maintenir un ensemble disjoint d'adresses IP .un nœud A désire d'entrer au réseau, demande une adresses a partir de ses voisins .qu'il peuvent l'attribue a nouveau une adresse, sans aucune contestation d'autres nœuds dans le réseau .le processus de fonctionnement de ce système est comme suite :

1. au départ, un seul nœud dans le réseau qui contient toute la plage d'adresses IP.
2. quand un nœud A (non configuré), désire de joindre au réseau, elle interroge le nœud le plus proche voisin configuré B, pour une adresse IP, le nœud B assigne une adresse IP parmi ces plage d'adresse, puis partage la plage d'adresse en deux groupe, et affecte un groupe au nœud A.
3. un nœud quitte le réseau d'une façon volontaire ou involontaire, quand un nœud quitte le réseau volontairement elle transmit sa plage d'adresses vers un nœud proche B, le nœud B devient avoir la responsabilité d'assignement ces nouvelles adresses IP, dans l'autre cas quand le nœud quitte le réseau d'une façon brusque, cette situation engendre une perte d'une plage d'adresse ce qui nécessite une synchronisation périodique entre les nœuds afin de récupère les plages d'adresses perdus
4. les nœuds synchronisent de temps en temps afin de et détectent s'il y a une perte d'un bloque d'adresse, chaque nœud dans le réseau maintien une table qui indique le bloque d'adresses contrôlé par chaque nœud (table ci-dessous)

Noeud ID	Adresse IP
1	0 – 31
3	42 – 63
5	36 – 128
……	…….

Si un nœud *A* reçoit une demande d'assignement d'adresse d'un autre nœud *B,* et si le nœud A affecte toute sa plage d'adresse, il diffuse une requête vers tous les nœuds du réseau pour obtenir une autre plage pour satisfait les futur besoins, le nœud qui contient le plus grand plage répond à cette requête en transmis une plage, et donc le nœud A peut configure l'adresse du nœud B

Quand un nœud quitte le réseau, ou une division dans le réseau, il y a des adresses s'utilisent par des nœuds qui ne fait partie du réseau, un mécanisme de synchronisation pour récupère ces adresses. Ce processus implique chaque nœud diffuse sa plage d'adresses IP

.cette diffusion est utilise par chaque nœud dans le réseau afin de mettre à jours ces plage d'adresses

6.2 Schémas statless (sans état) :

Dans ce schéma chaque nœud prend l'initiative de configurer soit-même, sans l'intervention d'aucuns autres nœuds, le rôle des autres nœuds résume seulement dans la participation dans le processus DAD pour protéger leurs adresses contre un usage accidentel

6.2.1 Détection d'adresses dupliquées basé sur requête

Perkins [5] propose une solution dans une Internet draft .cette solution performe une DAD à travers plusieurs tours elle s'appel query-based DAD (QDAD). QDAD basé sur le même mécanisme d'auto-configuration des adresses dans IPv6. Si un nœud *X* veut adhérer au réseau, elle choisit arbitrairement une adresse IP. Un message AREQ (Address Request) le but de AREQ est de trouver un chemin vers un nœud avec l'adresse spécifié .si l'adresse choisi est déjà attribué à un nœud un message AREP (Address Response) retourne vers le nœud *X*. l'absence d'un AREP au bout d'un temps indique qu'aucun nœud assigné cette adresse choisi par *X*. dans l'autre cas le Nœud *X* choisit aléatoirement une autre adresse et relance cette procédure encore

6.2.2 Passive DAD :

La fusion de plusieurs réseaux ad hoc, peut engendre un conflit d'adresses entre les nœuds de différent réseaux, un processus de détection de conflit tel que DAD est indispensable dans cette situation pour chaque nœud. Le volume du trafic généré par le DAD est proportionnel avec le nombre nœuds dans chaque réseau. Ce qui dégrade la performance du réseau et augmente la consommation de la bande passante disponible .Le but du PDAD est la détection des conflits sans génère un trafic supplémentaire, en exploitant les propriétés des protocoles de routage existant [7]

Dans la catégorie des protocoles de routage basent sur l'état de lien, chaque nœud informe périodiquement ses voisins, PDAD essaye d'exploite ces propriété sans utilise un mécanisme spécifie pour la détection des conflits. Les auteurs proposent trois approches chacune s'articule sur une propriété du protocole de routage à état de lien

1) **PDAD –SN :** Chaque nœud utilise le Numéro de Séquence NS une seul fois pendant une période de temps T_d, d'une manière incrémentale, et seulement une seule fois dans ses diffusions. Les nœuds base leurs routages sur l'état de lien, ne routent pas les messages dont la valeur du NS plus petite que ceci stocké dans leurs tables.

La non duplication d'adresses repose sur deux théorèmes, si l'un n'est pas vérifié, un conflit d'adresse existe dans le réseau :

Théorème (1) : deux messages ave le même NS et adresse source sont des copies du même message.

Théorème (2) : un nœud n'a jamais reçu aucun paquet d'état de lien avec son propre adresse et un Numéro Séquence plus grand que celle la valeur du compteur.

Selon le théorème (2) : peut détecter un conflit s'il reçu un message avec comme une adresse source, et un NS plus grand que son propre valeur (figure 5).

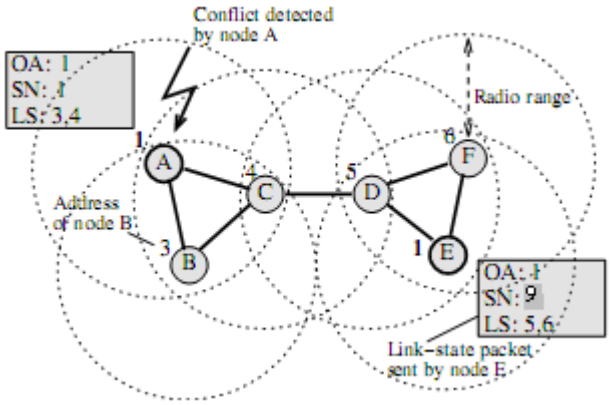


Figure 3.5 : Résolution du conflit basé sur PDAD-NS

Si le nœud A reçu un message, de nœud E qui porte la même adresse mais avec une valeur de NS plus grande que celle du A, il résulte qu'il y a un conflit d'adresse avec le nœud E.

Grâce a ces deux théorèmes tous les conflits d'adresse, peuvent résolu .à condition que les nœuds qui ont la même adresse n'ont pas les même voisins (la distance entre eux plus de deux sauts)

L'autre approche PDAD-LP le facteur que les nœuds déplace avec une vitesse limité peut exploiter, d'habitude la fréquence de mis à jour des tables est ajustée selon la vitesse maximale des nœuds La troisième approche, PDAD-NH "Neighborhood History", exploite la propriété que chaque nœud conserve l'historique de ces voisins. (Figure 6) Si le nœud A reçu un message d'état de lien de nœud F, qui est le voisin du E, le nœud F n'est pas un voisin, A conclu qu'il y a une duplication d'adresse avec autre nœud.

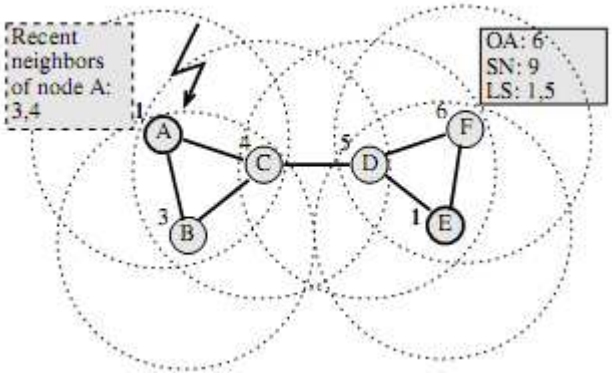


Figure 3.6 : Résolution du conflit basé sur PDAD-NH

Ces trois approches sont testées avec des protocoles de routage à état de lien, tel que OLSR, FSR, une application ultérieur de cette approche avec le protocole réactif AODV est présentée dans [10]

6.3 Schémas Hybride:

PACMAN (Passive AutoConfiguration for Ad hoc Mobile Networks) décrit dans [9] il utilise une solution hybride les éléments de deux approche "Statfull" une gestion lente des table adresses assignées dans le réseau, ce qui préserve a bande passante et "Statless " pour l'assignement d'adresse.

PACMAN génère assez trafic de contrôle car sa conception basé sur une sous couche plus efficace, qu'une conception indépendant au protocole de routage pour l'assignement d'adresse

il utilise un algorithme probabiliste, son architecture Modulaire (figure 6) permet facile à l'intégration dans des nouveaux protocoles de routage.

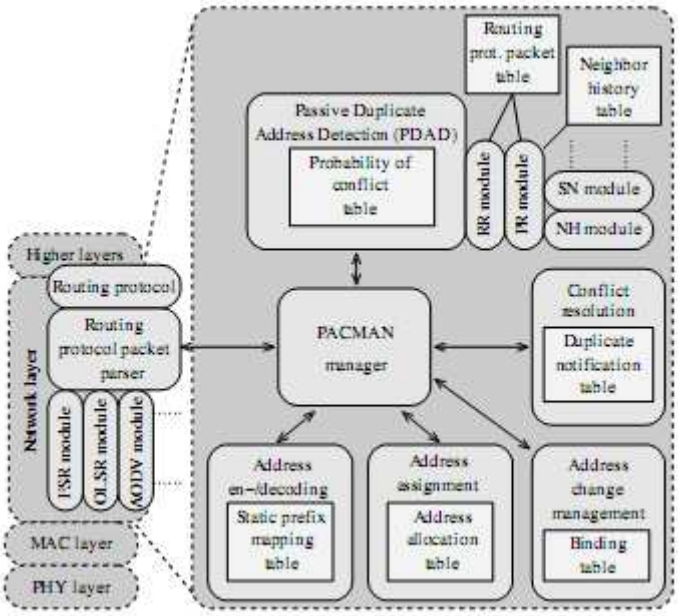


Figure 3.7 : Architecture modulaire du PACMAN

Le module "Address assignment" son rôle assigne une adresse aléatoire au nœud utilisant un algorithme probabiliste, basé sur une estimation sur le nombre des nœuds et une table des adresses allouées. Cet algorithme calcule un espace adressage, et choisir arbitrairement une adresse à partir de cet espace assurant que cette adresse ne fait pas parti de la table des adresses allouées. Le module PDAD [7] est reprendre pour la détection des conflits dans le cas où il a une fusion avec d'autres réseaux sans génère un trafic supplémentaire, dans cette approche le processus PDAD peut fonctionne avec les deux protocoles réactif ou proactif.
Un module optionnel "codec d'adresses" permet une compression de la taille d'une adresse,

7. Conclusion :

Un réseau ad hoc est un réseau auto configuré dans le sens où tous les nœuds acquises une adresse IP sans l'intervention d'une entité centrale, les nœuds eux-mêmes explicitement contribuent dans cette opération par l'attribution d'une adresse IP à chaque nouveau nœud désire d'entrer dans le réseau, un réseau ad hoc est subit à certain événements tel que la fusion de plusieurs sous-réseau en un seul réseau, la fusion peut engendrer une situation où des nœuds portent la même adresse ce qui nécessite un mécanisme garantissant l'unicité de toutes les adresses existent dans le réseau, dans ce chapitre nous présentons différents catégorie d'allocation d'adresses, détection de conflit ou sans détection de conflit, un schémas qui peut combine les deux qui est le schémas hybride.

Référence :

[1] R.Droms. "*Dynamic host configuration protocol*.", RFC 2131, IETF Mars 1997.

[2] H. Kumar, R.K. Singla, S. Malhotra "*Issues & Trends in AutoConfiguration of IP Address in MANET*" Vol. III (2008), Suppl. issue: Proceedings of ICCCC 2008, pp. 353-357

[3] M.Mohsin , R.Prakash "*IP address assignment in a mobile Ad-hoc network*" IEEE MILCOM 2002

[4] S.Nesargi, R.Prakash. MANETconf: "Configuration of hosts in a mobile ad hoc network" .In Proc .of IEEE INFOCOM 2002, Juin 2002

[5] C. E. Perkins, E. M. Royer, S.R. Das "*IP address autoconfiguration for ad hoc Networks*". (IETF), Internet Draft, http://people.nokia.net/ charliep/txt/aodvid/autoconf.txt, November 2001

[6] Duplicate MAC Addresses on Cisco 3600 Series, http://www.cisco.com/warp/public/770/ 7.html, 1997.

[7] K. Weniger "*Passive Duplicate Address Detection in Ad hoc Networks*" In Proc. of IEEE WCNC 2003, New Orleans, USA, March 2003

[8] S.Misra, IWoungang and S. C Misra "Guide to wireless ad hoc networks" springer 2008

[9] K. Weniger. "*PACMAN: Passive autoconfiguration for mobile adhoc networks*". In IEEE JSAC, Special Issue on Wireless Ad Hoc Networks, January 2005.

[10] R. Hinden, S. Deering "IP Version 6 Addressing Architecture" RFC 2373 IETF http://www.ietf.org/rfc/rfc2373.txt

Chapitre 4 :

Les protocoles de niveau transport pour les réseaux ad hoc

1. Introduction :

Selon le model TCP/IP un réseau est organisé d'une manière hiérarchique, où chaque couche représente un aspect spécifique du réseau. La couche transport c'est la plus compliqué entre eux [1], car elle joue un rôle intermédiaire entre les couches basses et les couches hautes, ainsi elle masque les détails d'implémentation des sous-réseaux aux couches hautes. Les protocoles usuels de transport de l'information dans les réseaux IP sont TCP (Transmission Control Protocol) et UDP (User Datagram Protocol), des statistiques affirme que 80 % du trafic Internet est basé sur le protocole de transport TCP [5].

Pour répondre aux nouveaux besoins qui n'existent pas au sein du protocole TCP ou UDP, l'IETF a élaboré un protocole spécifique s'appelle le SCTP (Stream Control Transmission Protocol), défini dans les documents Internet [2], [3], [4] le but initial de ce protocole est le transport de la voix sur les réseaux IP, SCTP hérite les mêmes caractéristiques du TCP (contrôle de flux, gestion des congestion, …), ainsi il porte de nouveaux concepts tel les cookies, le multistreaming et le Multihoming. Le système des cookies permet de sécuriser les connexions SCTP face aux différents types d'attaques, tandis que le multistreaming peut résoudre le problème des arrivées hors séquence et le blocage dans les buffers de TCP, le multihoming pour un but de créer une redondance au niveau transport par des équipements qui multi-cartes. L'idée de multihoming commence dans les années 2000, les administrateurs des sites web attachent leurs sites par plus d'une connexion Internet chacune avec un fournisseur différent, on parle un "site multihomed" le but initial de cette idée est la prise en charge des accès du public Internet, et l'augmentation de la tolérance aux pannes, en cas d'une défaillance d'une connexion le site reste accessible via l'autre, d'autre recherches en cours pour exploite cette technique tel que sur la répartition de la charge en cours.

Dans un cadre ad hoc, les protocoles de transport montrent un comportement inattendu à cause de la mobilité des nœuds et le taux d'erreur élevé [5]. C'est ce problème que nous nous sommes proposes d'étudier. Dans ce chapitre avant d'investir dans le protocole SCTP, on présente le TCP avec quelques notions communes avec SCTP et les clés essentielles à la compréhension de la problématique de la couche transport dans les réseaux ad hoc

2. Le protocole TCP

TCP est un protocole de bout-en bout, opère indépendamment aux caractéristiques de sous-réseau, il été spécifier dans le document RFC 793, il est défini dans le but de fournir un service de transfert de données de haute fiabilité entre deux noeuds raccordés sur un réseau de type "paquets commutés", et sur tout système résultant de l'interconnexion de ce type de réseaux [1]. Cette fiabilité s'appuie sur l'utilisation des acquittements (ACK) et des numéros de séquence, Ainsi par un multiplexage, TCP spécifie comment distinguer plusieurs connexions sur une même machine par utilisation de la notion abstraite ***de port***, qui identifie une destination particulière dans une machine [2], les caractéristique principaux du TCP sont suivantes :

- **protocole bout en bout** : tout le contrôle de la connexion réside uniquement chez l'émetteur et le récepteur (indépendant aux caractéristiques des sous-réseaux).Figure 1.4

- **orienté connexion** : avant tous transfert des données une phase de connexion doit être établie entre les deux entités communicantes, dés que les deux entité terminent leurs dialogue une phase prend de place c'est la phase de fermeture de la connexion.
- **Fiable** : c'est-à-dire que le TCP assure la délivrance de la totalité des paquets de façon ordonnée et exemptée d'erreurs.
- **Contrôle de flux** : pour éviter des engorgements du récepteur, l'émetteur adapte le nombre de paquets envoyés à la taille du buffer de réception, quand le récepteur retourne un ACK confirmant la bonne réception ce ACK contient le nombre d'octet qu'il peut recevoir dans le prochain fragment TCP.
- **contrôle de congestion :** c'est un mécanisme qui s'active lorsqu'il y a une saturation dans les équipements de routage du réseau.

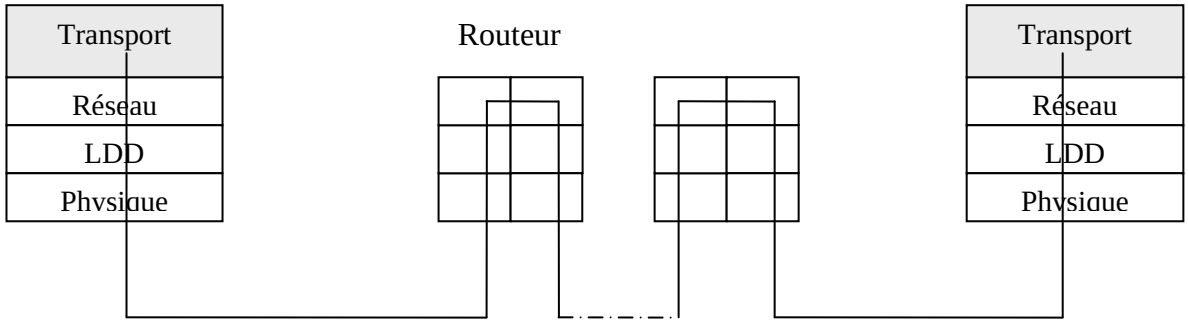


Figure 4.1 le concept de bout en bout

L'autre protocole de transport est le UDP, plus simple que TCP, il est décrit dans le document RFC 768 Ce protocole définit une procédure permettant à une application d'envoyer un message court à une autre application, UDP est un protocole non fiable parce qu'il ne garantit ni la délivrance du message, ni la détection d'une éventuelle duplication. Les applications qui nécessitant une transmission fiabilisée et ordonnée d'un flux de données implémenteront de préférence le protocole TCP.

3. les Mécanismes pour la fiabilité des transmissions :

Pendant la phase de transferts de données, certains mécanismes clefs permettent d'assurer la robustesse et la fiabilité de TCP. En particulier, les numéros de séquence sont utilisés afin d'ordonner les segments TCP reçus et de détecter les données perdues, les checksums permettent la détection d'erreurs, et les acquittements, ainsi que les temporisations, permettent la détection des segments perdus ou retardés.

3.1 Acquittements ACK (Acknowledgments) :

TCP utilise la technique de l'accusé de réception, lorsque un destinataire reçoit un paquet valide il retourne un accusé ACK confirme la bonne réception du paquet, ainsi l'émetteur sait si l'information qu'il voulait transmettre est bien parvenu au destination, ces ACK peuvent être immédiat ou cumulatif. Ainsi que chaque segment TCP porte un *checksum* calculé auparavant par l'émetteur contrôle des erreurs éventuelle le récepteur utilise pour vérifier la validité des données transmis. une fois les ces données arrive intact, le destinataire doit acquitter les segments reçus en indiquant qu'il a reçu toutes les données du flux d'octets jusqu'à un certain numéro de séquence.

Une option s'ajoute au TCP afin d'éviter des retransmissions inutiles (si un paquet perdu d'un bloc), nommée acquittement sélectif (Selective ACK ou SACK) RFC 2018, cette option est négocie lors de l'établissement de connexion elle permet à la destination de sélectionner et préciser le paquet à retransmettre

3.2. Contrôle de flux :

L'objectif d'un mécanisme de contrôle de flux est de cadencer l'envoie des paquets entre un émetteur rapide et un récepteur lent, pour cela TCP ajuste ces transmissions à travers un système de fenêtre glissante. TCP définit le nombre de paquets pouvant être envoyé sans être acquitté, cette fenêtre est appelé TWND (Transmission Window), la fenêtre de transmission TWND est alors régie par la formule :

$$TWND = Min(CWND, AWND) \quad \text{.....(1)}$$

- **AWND** (Avertised Window) : elle permet au récepteur d'annonce le nombre de segments qu'il est capable actuellement de recevoir, sa valeur dépend de l'espace dans son buffer et de sa vitesse de traitement les paquets reçus.

- **CWND (Congestion Window)** : La fenêtre de congestion cwnd indique la quantité maximale de données que l'émetteur peut envoyer sur le réseau avant de recevoir un acquittement. Sa valeur varie dans le temps selon le mécanisme de contrôle de congestion, son comportement est détaillé dans la section suivante

3.3. Temporisation et retransmission :

Afin d'atteindre une bonne fiabilité, une entité TCP envoie un paquet et attend son acquittement, si au bout d'un temps RTO (Retransmission Time Out) l'émetteur ne reçoit pas un accusée de réception, il décide de retransmettre le paquet, ce délai doit être supérieur au RTT (Round Trip Time) : c'est-à-dire le temps écoulé entre l'émission d'un paquet de données et la réception de son acquittement respectif. Du fait de la grande variété de réseaux, la valeur de temporisation de retransmission .*RTO* doit être déterminée dynamiquement

$$SRTT = (1-\alpha) * SRTT + \alpha * RTT \quad \text{.....(2)}$$, avec α =7/8

$$RTO = RTT\ moyen + 4 * Var(RTT) \quad \text{.....(3)}$$

4. Contrôle de congestion :

Le contrôle de congestion est une caractéristique majeure du protocole TCP. Il est utilisé pour atteindre de hautes performances et éviter l'effondrement du réseau Le mécanisme de contrôle de congestion essaie de maintenir le taux des données entrant dans le réseau en-dessous du taux qui cause une congestion.

4.1 Les mécanismes de contrôle de congestion :

TCP utilise un certain nombre de mécanismes afin d'obtenir une bonne robustesse et des performances élevées. Ces mécanismes comprennent l'utilisation d'une fenêtre glissante, l'algorithme de démarrage lent (*slow start*), l'algorithme d'évitement de congestion (*congestion avoidance*), les algorithmes de retransmission rapide (*fast retransmit*) et de récupération rapide (*fast recovery*), etc. Des recherches sont menées actuellement afin d'améliorer TCP pour traiter

efficacement les pertes, minimiser les erreurs, gérer la congestion et être performant dans des environnements mobiles.

a) Slow start et congestion avoidance

Un émetteur TCP utilise L'algorithme *"slow-start and collision avoidance"* afin de réguler le nombre de paquets injecté, et deviner l'état réseau, son principe consiste à débuter d'une fenêtre de taille égale à 1 et à augmenter la taille de cette fenêtre d'une façon exponentielle chaque fois que l'ensemble des paquets de la fenêtre a été bien reçu, jusqu à atteindre la taille de RWND (fenêtre de réception) ou recevoir un signe de la saturation dans le réseau [13]. C'est la phase de départ lent. Ce schémas répète, mais cette fois s'arrête à une certaine valeur (SSThreshold = MIN (CWND, RWND) / 2) de CWND inférieur au denier pic où le paramètre CWND va maintenant augmenter de façon linéaire (Eq.4.4) c'est la phase d'évitement de congestion, elle est moins

$$CWND = CWND + \frac{MSS * MSS}{CWND} \quad \cdots\cdots\cdots\cdots\cdots\cdots (4)$$

MSS (Maximum Segment Size) : la taille maximal d'un paquet pouvant transiter un réseau sans être fragmenté

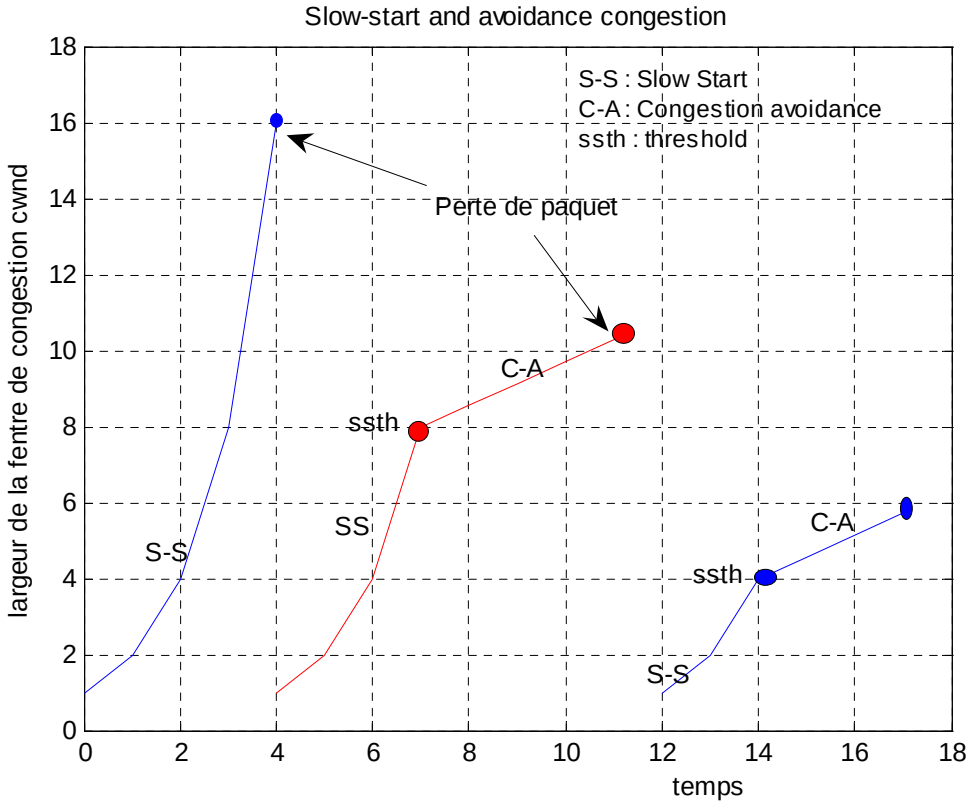


Figure 4.2 Fonctionnement de l'algorithme slow-start and collision avoidance

b) Explicite Congestion Notification :

ce mécanisme Venu du monde filaire, le ECN "Explicite Congestion Notification**"** permet à un noeud routeur, selon l'occupation moyenne de son buffer, de positionner un bit dans l'entête IP du paquet qu'il est en train de traiter, pour signaler qu'une congestion est probable. Le paquet, en arrivant au récepteur de la connexion TCP va positionner le bit ECN-echo dans quelques-uns des acquittements suivants.

L'ECN-echo va avoir pour effet d'inhiber l'accroissement de CWND à l'arrivée de l'acquittement au niveau de l'émetteur TCP, dans [13] les auteurs montrent qu'un réseau ad hoc utilise l'option ECN atteint de bonnes performances en prévenant la congestion.

5. Problèmes de TCP dans les réseaux ad hoc :

Des études récente [5],[6], ont indiqué que les performances de TCP se dégrade d'une manière significative dans les réseaux mobiles ad hoc, Les principales raisons qui entraînent cette dégradation proviennent, de la qualité du lien sans fil et, la qualité du chemin multi-hop. Plus précision c'est que TCP est incapable de distinguer entre perte des données causer d'une congestion de réseau ou d'une rupture du lien, ainsi TCP considère que toute perte de paquets ou de retard comme un signal de congestion [3],[4],[5] donc TCP exécute le mécanisme de contrôle de congestion d'une manière systématique, bien que les MANET rencontre plusieurs types de pertes et de retard qui ne sont pas liés à la congestion.

Sur NS2 "Network simulator", on étudie l'effet du nombre de sauts sur le nombre de paquets reçu par chaque nœud, La figure 4.4 montre la topologie et la distribution des nœuds sur le NAM "Network Animator" du NS2.

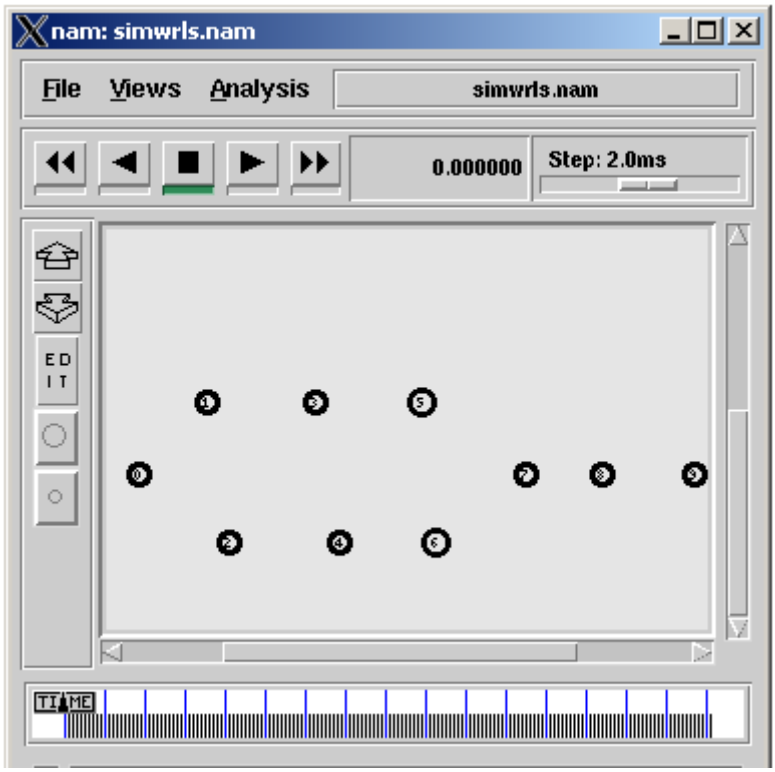


Figure 4.3 : Topologie du réseau

Dans cette simulation on utilise une architecture client/Serveur, où le nœud (0) joue le rôle d'un serveur FTP, tandis les autres nœuds (1..9) sont des clients, d'autre coté pour assuré que les paquets arrivent aux différents nœuds d'une manière saut-par-saut, on distribue les nœuds sur la surface avec une distance uniforme et une faible mobilité. Les différents paramètres sont décrits dans la table suivante :

Application	FTP
Protocole de transport	TCP
Protocole de routage	AODV
Mobilité	Faible
Nombre de nœuds	10
Surface de la simulation	800 x 800 m^2
Distance entre les nœuds	Constante

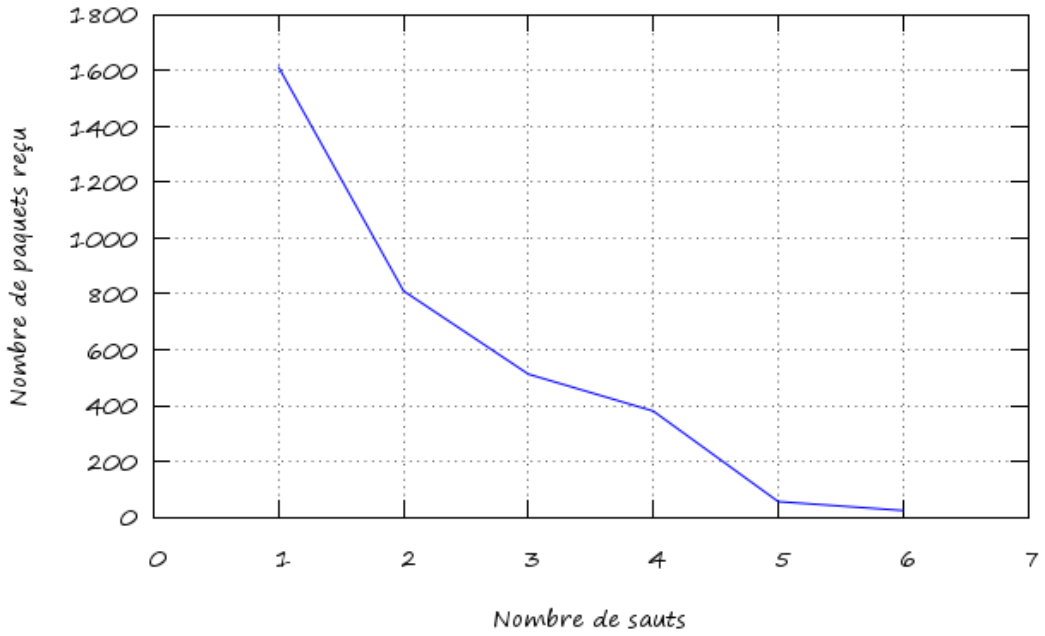


Figure 4.4 l'influence de longueur de chemin sur le nombre paquets reçus

Analyse dés résultats :

On voit qu'il y a une chute massive sur de nombre de paquets reçus, tandis la distance augmente des nœuds au serveur, cela revient, le protocole de routage utilisé AODV, qui crée les route à la demande, ainsi le temps de traitement des paquets chaque passage de données ou un acquittement. D'autres facteurs qui chutent les performances du TCP dans les réseaux ad hoc, les collisions, compétition d'accès au médium ou encore problème de nœud caché, ces problèmes assurent que la fenêtre de TCP, *TWND* figure 4.6 reste trop petite provoquant un baissement inutile du débit de transmission et une grossière du RTO.

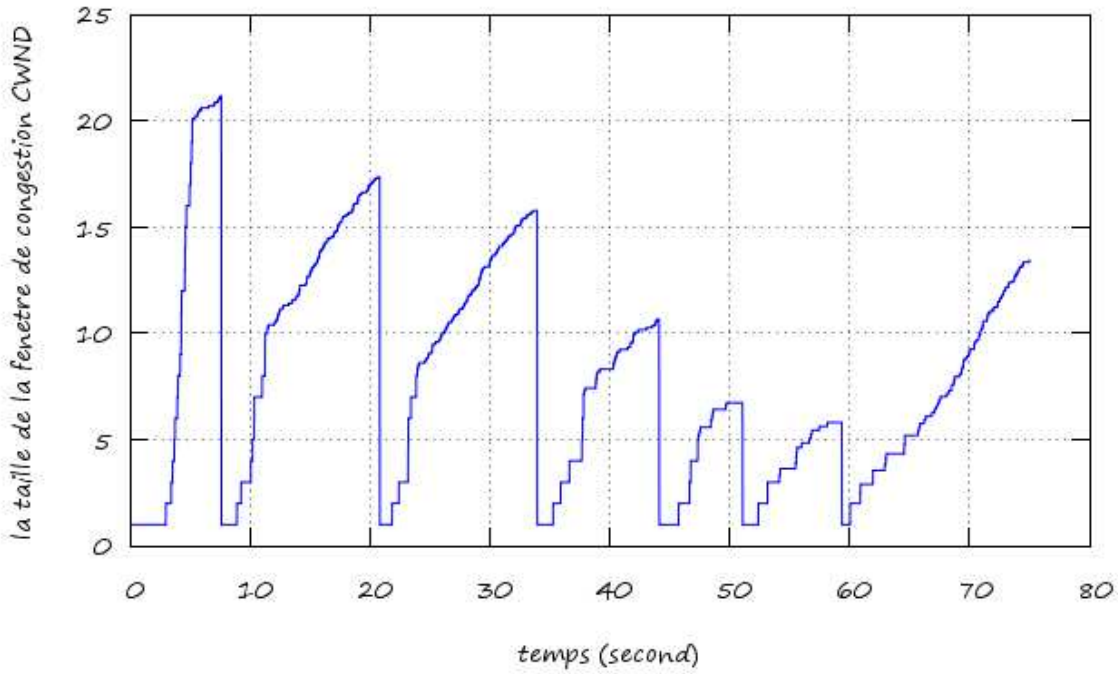


Figure 4.5 : comportement de la fenêtre de congestion dans un réseau ad hoc

6. Les solutions proposées pour améliorer le TCP pour les réseaux ad hoc :

Afin d'adapter le protocole TCP dans les réseaux ad hoc des améliorations amenées par les chercheurs au protocole TCP, on classifié ces propositions en deux catégories selon la taxonomie proposé dans [11] : celles aux extrémités de la communication c'est-à-dire entre l'émetteur et le destinataire, et celles où elle est implémente dans tous les nœuds du réseau.

6.1 Les approches distribués "feed-back" :

Dans ces approches, le réseau met en œuvre un mécanisme de surveillance qui génère un message de notification quand il détecte un événement anormal alors que le protocole TCP peur réagir par des les mécanismes appropriés

a) ATCP :

ATCP (Ad hoc TCP), proposé par Liu et Singh [7] Le principe de cette approche est d'inclut une "cross layer" entre la couche TCP et la couche IP au niveau de l'expéditeur, qui a pour but de filtrer les signes de congestion émanant du réseau, cette couche surveille l'état du TCP et du réseau, qui sont connu grâce à des messages d'ECN (Explicit Congestion Notification) et des messages ICMP (Internet Control Message Protocol), de ce fait la couche ATCP met l'agent TCP dans l'un des état approprié (persistant, contrôle de congestion ou retransmission) qui correspond respectivement à la rupture de lien , congestion de réseau ou un BER élevé. De son coté ATCP définit quatre états : "normal", "congestionné, "perte", ou "déconnexion". La congestion est détecte grâce des messages ECN elle met l'expéditeur TCP dans l'état persistant, fixe la fenêtre de congestion TCP (cwnd) à un.

b) TCP-BuS

(TCP Buffering capability and Sequence information) Le principe de cette approche c'est l'utilisation des buffers au niveau de chaque nœud .Quand un noeud "PN : Pivoting

Node" [8] détecte une rupture du chemin, il retourne un message de contrôle "ERDN" vers la source, indiquant la rupture de la route, ce message contient le numéro de séquence du segment TCP. Tous les nœuds intermédiaires mémorisent les paquets en cours dans ses buffers, dés que lae nœud source reçoit ce message arrête son émission, jusqu'à la réception d'un autre message " ERSN" qui indique le rétablissement de la route. Le nœud PN c'est lui qui prend la charge de rétablir la route. TCP-BuS, a montré de bons résultats au vu des échecs de routage en atteignant 30% de débit supplémentaire en moyenne par rapport à TCP

c) Split TCP :

Les auteurs dans [9] proposent une autre approche pour améliorer les performances du TCP dans les réseaux ad hoc en terme de fairness et de throughput. Le principe de cette approche réside dans le découpage d'une long connexion TCP en petits segments localisé le protocole élit des nœuds s'appelle Proxy, Un Proxy intercepte les fragment TCP, mémorisent et l'acquitté vers la source (ou Proxy précédent) par un acquittement local LACK, ainsi un Proxy délivré un paquet à un débit adéquat, afin de respecte le bout en bout le destinataire retourne un ACK vers la source confirmant la bonne réception de ces paquets.

6.2 Les approches bout en bout :

Les approches end-to-end ne demande aucune implémentation dans les nœuds intermédiaires, seuls les entités extrémités da la connexion sont concernés par l'état du réseau.

a) TCP-DOOR :

Dans une session TCP idéal les paquets de données sont arrivées au récepteur en séquence et dans l'ordre. Cependant pour les réseaux ad hoc un phénomènes fréquente (out-of-order : OOO), TCP DOOR [11] (Detection of Out-Of-Order and Response) est proposé afin d'agir à ce type de problème, du de la mobilité des nœuds et changement fréquente de la route. Les auteurs assimilent qu'un OOO est probablement causée par les changements de route et non par la congestion

La détection du hors séquence est effectuée, au niveau de l'émetteur, sur les acquittements et, au récepteur, sur les données, quand un émetteur reçoit un ACK porte des numéros de segment moins d'un ACK précédente, il déduit qu'un OOO aura lieu. Le récepteur soit par grâce à une nouvelle technique de numérotation une façon pour réalise ajouter à l'entête TCP un TPSN "TCP Packet Sequence Number˝ ce TPSN marque l'ordre exacte de chaque fragment TCP (dans le TCP de base le numéro n'est pas incrémenté lors des retransmission) l' autre méthode peut facilite la détection des paquet OOO sans modification dans la structure de TCP, un émetteur précise le temps exacte dans l'entête de chaque fragment TCP envoyée, ceci permet au récepteur de déduire s'il y a un OOO, en comparant les "timestamp˝ dans deux paquets consécutifs.

Lorsque le récepteur détecte un OOO sur les données reçus, il signale a l'émetteur en positionne un flag dans un paquet ACK, de même l'émetteur vérifie chaque ACK en cas de détection de hors séquence l'émetteur dispose de deux mécanismes, l'un de bloquer le contrôle de congestion qui est indésirable dans cette situation, l'autre d'accélérer le recouvrement d'errer.

b) ADTCP :

C'est une approche bout en bout [11], le but de cette approche est de prendre une robuste décision face aux différents événements pour cela, les auteurs proposent la mesure de plusieurs métriques au niveau de récepteur, détecter l'état du réseau (congestionné, Erreur du canal, changement de route ou Déconnexion) et prendre la réaction adéquate pour chaque situation, pour détecte la congestion recommande de mesurer quatre métriques sont mesurées au niveau du récepteur pour identifier l'état du réseau

- **IDD (Inter-paquet Delay Difference)** : représente le délai entre deux transmissions consécutives le niveau de congestion
- **STT (Short-terme Throughput)** décrit le nombre de paquet dans un intervalle T, qu'il diminue lors d'une congestion dans le réseau.
- **POR (Paquet Out of Order):** cette métrique augmente en cas de changement de la route
- **PLR (Paquet Loss Ratio)** : représente le ratio des paquet OOO reçus

Si l'une des mesures n'est pas claire pour la décision, utilise une combinaison de ces métriques pour avoir un indicateur de congestion robuste, ainsi de réduire la probabilité d'une fausse détection, les deux premières métriques sont combinées pour avoir un indicateur de congestion, les deux dernières sont utilisées pour détecter respectivement le changement de la route et les erreurs du canal de transmission.

À l'arrive de chaque paquet, le récepteur calcule les quatre métriques ci-dessus, et estimer l'état du réseau, puis il inclut cette l'information sur le réseau dans l'acquittement vers le expéditeur avec chaque acquittement. En conséquence L'émetteur peut prendre l'action appropriée

7 le protocole SCTP (Stream Control Transmission Protocol)

7.1 Introduction

Le but initiale de SCTP a été conçu un protocole plus robuste pour transporter les messages de signalisation sur des réseaux IP VoIP (projet SIGTRAN de IETF) [14], récemment des développements le rend largement utile pour le transport des divers applications web et le devient un la standardisation Transport Area Working Group TSVWG de IETF en 2001

Plusieurs protagoniste du marché de télécommunication et de l'informatique (Nokia , Cisco , HP, ericsson..) sont intéressé par ce nouveau protocole [16], car il fournit un concept de transmission des données complètement neuf , basé sur des flux .il est beaucoup plus flexible comparé à ses prédécesseurs TCP et UDP .comme on peut le constater dans les diverses études faites sur ce protocole, son application ne se limitera pas uniquement de la signalisation , mais aussi au transport d'application multimédias

7.2 Présentation :

SCTP est un protocole orienté connexion fonctionnant au dessus d'un protocole non orienté connexion comme IP. SCTP offre un service de transfert de données fiable, garanti par une gestion des erreurs à l'aide d'accusée de réception, et un non duplication des datagrammes. Les détections de corruption, de perte et de duplication des données sont effectuées par des

mécanismes de checksum et de numéro de séquence. Une retransmission sélective des datagrammes est appliquée lors de la perte ou de la corruption des données

Similaire au TCP la conception de SCTP inclut des propriétés comme la prévention des congestions et la résistance aux attaques de type SYN, la différence majeur entre SCTP et TCP est le concept de Multihoming (hôte dote plusieurs interfaces réseau) et le multistreaming (plusieurs flot dans une connexion) à travers une seul connexion

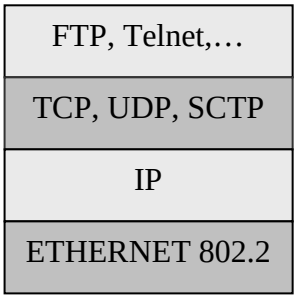


Figure 4.6 : SCTP dans la pile du protocole IP

7.3. Fonctionnement de SCTP :

Le service de transport SCTP comme décrit dans RFC [2960], peut être décomposé en blocs chacun assure une fonction distinct, représenté dans la figure

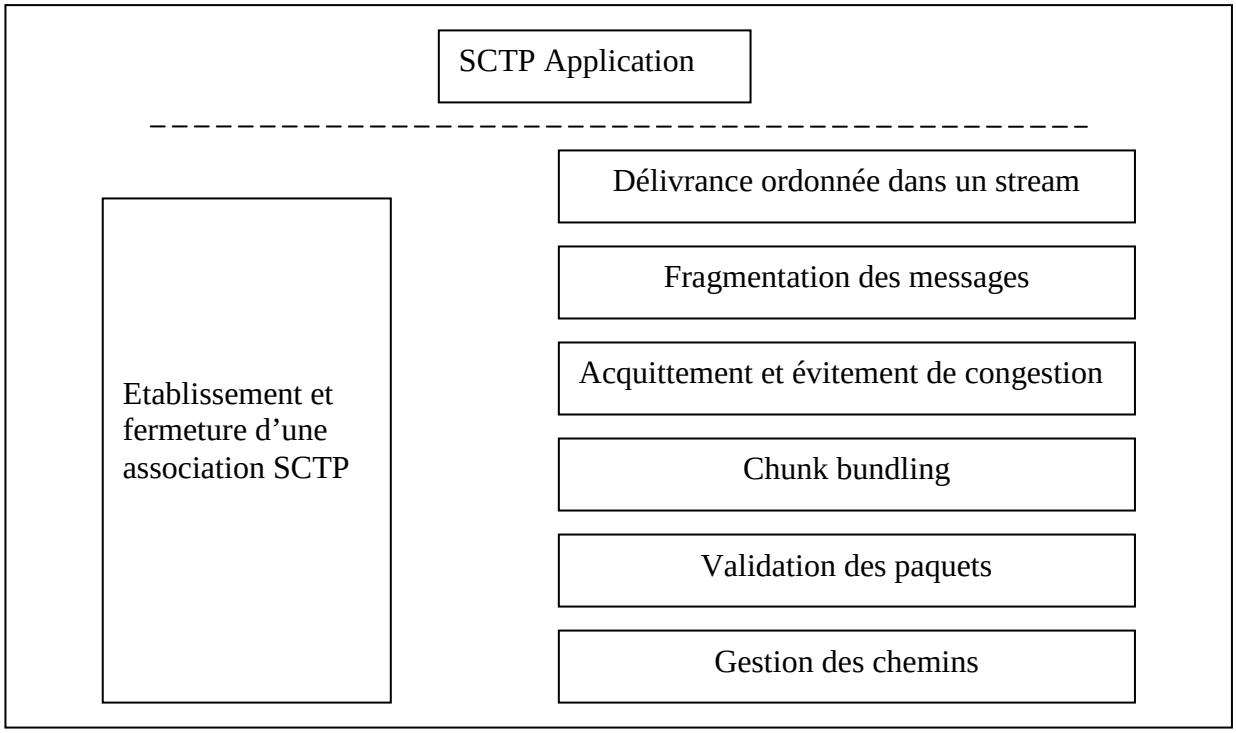


Figure 4.7 Fonctionnement de base de SCTP

1. Etablissement et fermeture d'une association:c'est l'une des spécifique de l'orienté connexion, avant qu'un transfert aura lieu une d'établissement de connexion est indispensable, et se termine par une phase de libération de connexion.

2. Délivrance ordonnée dans un stream : un stream dans le contexte de SCTP se réfère à une séquence de messages utilisateurs. Une association de SCTP peut soutenir de multiples streams.
3. Chunk bundling : cette fonction gère l'assemblage du paquet SCTP et son réassemblage lors de la réception.
4. Fragmentation des messages: SCTP fragmente les messages utilisateur pour s'assurer que la taille des paquets passés à la couche inférieure ne dépasse pas le MTU (Maximum Transmission Unit). Les fragments reçus sont réassemblés avant d'être transmis à la couche supérieure.
5. acquittement et évitement de congestion : conformément au TCP, chaque paquet SCTP identifie par un numéro unique indépendant au numéro de stream, la bonne réception d'un paquet doit être suivi par un acquittement,
6. Validation du paquet: protection des attaques de sécurité et des paquets de SCTP "périmés"provenant d'une association antérieure
7. Gestion des chemins : dans le cas où les nœuds multi-homed, SCTP identifie un chemin primaire et plusieurs chemins redondante, SCTP procure un mécanisme pour contrôler l'état de chaque chemin que peut emprunter l'association.

7.4 Association SCTP :

Une association SCTP, est une relation de niveau transport entre deux entités SCTP, équivalent d'une connexion dans la littérature TCP, cette association est défini par le quadruple « adresse source, N° de port », « adresse destination, N° de port » dans le cas d'une connexion avec des hôtes "Multi-homed" figure une association est défini par l'ensembles des adresses IP de chaque hôte « IP1, IP2, N°port » et « IP4, N°port »

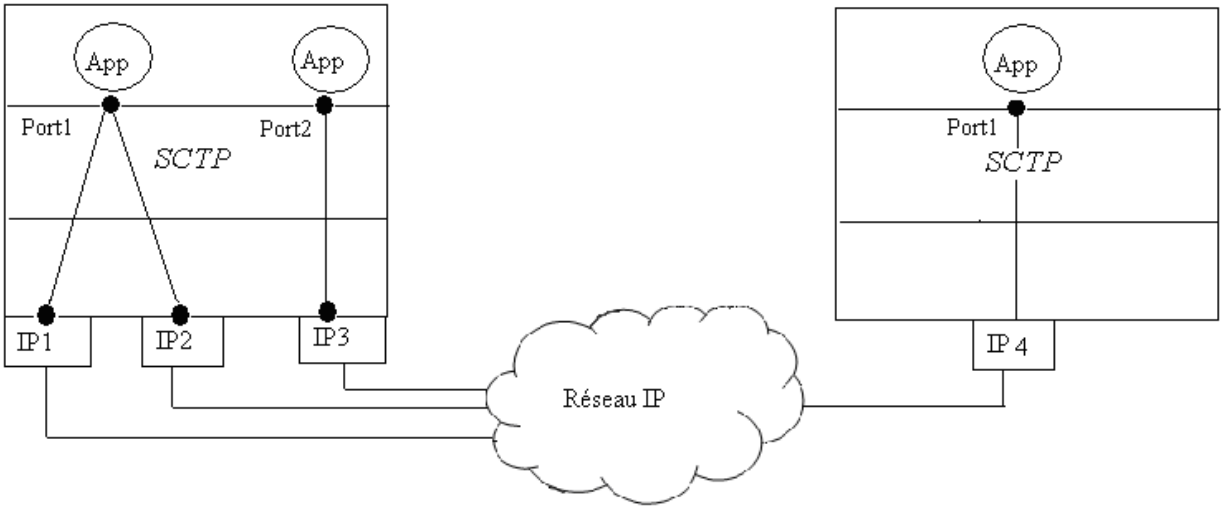


Fig 4.8 : Diagramme le concept d'une association SCTP

7.5 Caractéristiques du SCTP :

Ce protocole fut à l'origine développé pour la téléphonie sur IP, ou voix sur IP (VoIP), et possède certains attributs intéressants qui en proviennent. Le niveau de l'industrie VoIP

requiert une très haute fiabilité, ce qui veut dire une grande faculté de récupération pour gérer les différentes sortes de problèmes. Ci-dessous une liste des fonctionnalités de base de SCTP.

- **Transmission fiable**. SCTP utilise les sommes de contrôle et SACK pour détecter les données corrompues, endommagées, dupliquées ou réordonnées. Il peut ensuite retransmettre les données si nécessaire. C'est à peu près comme TCP, mais SCTP est plus tolérant pour le réordonnancement des données et permet un captage plus rapide.

- **Le Multi-streaming :** Cette caractéristique unique au protocole SCTP permet le multiplexage de plusieurs flux (streams) de données simultané dans un même flux, de nombreuses applications peuvent bénéficié de cette propriété technique, exemple les pages web animé, où chaque type de données est envoyé sur un stream distinct.
- **le Multihoming :** la propriété essentielle du protocole de transport SCTP est le support des nœuds avec des connexions multiples, c'est-à-dire des nœuds qui peuvent être atteints via plusieurs adresses IP. Le multi-homing spécifié dans le protocole SCTP sert uniquement pour la redondance, la répartition de charge ne fait pas partie de la spécifcation actuelle du protocole et reste toujours à l'étude. [21].
- **une large fenêtre de réception :** afin d'augmenter le débit de transmission cas des réseaux satellitaires, SCTP améliore la taille de la fenêtre de réception en 32 bit, contre 16 bit cas du protocole TCP
- **sécurisé au niveau transport :** le mécanisme des COOKIES, et la connexion en quatre phase, rend SCTP plus robuste aux éventuelles attaques existe dans le TCP

7.6 Format d'un message SCTP

L'unité de données protocolaire PDU du protocole SCTP, elle est composé d'un entête commun et d'un ensemble de CHUNKs (terminologie SCTP), plusieurs chunks peuvent multiplexé dans un seul paquet SCTP (figure 4.9), le nombre N de CHUNKs est déterminé par la taille du MTU "Maximum Transmission Unit", c'est-à-dire la taille maximal d'un paquet SCTP qui ne subit à aucune fragmentation [12] Un chunk peut contient des données utilisateur ou bien des données de contrôle, selon la valeur apporté par le champ *type*.

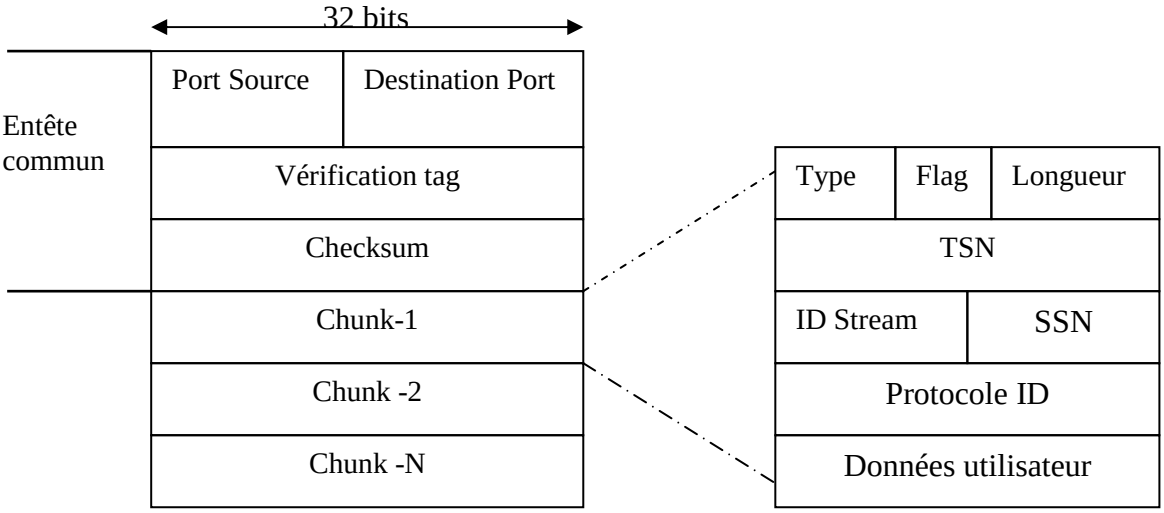


Figure 4.9 Format d'un paquet SCTP

- Port Source et Destination : les mêmes que dans TCP et UDP
- Type : Chaque chunk a un champ Type, qui permet d'identifier le transport des données et les information de contrôle. Les chunks ont une taille variable. Les principaux de chunks (extrait du RFC 2960) sont (cf. table 1):
- Checksum (32 bit contre 16 bits dans TCP) : ce champs est utilise pour corriger les erreurs éventuels qui peuvent subir un paquet SCTP lors de son trajet
- vérification tag : une information spécifique attaché à un paquet d'une association elle fournir une clé au récepteur afin de vérifier qu'un paquet SCTP, apartient à l'association courante et pas d'un paquet d'une ancienne association
- TSN (Transmission Sequence Number) : Pour des raison de fiabilité et contrôle de congestion chaque chunk, est assigné un identificateur le distinguer d'autres chunks

7.7 Quelque type chunks intéressant :

Chaque chunk a un champ type, qui permet d'identifier le transport des données et les informations de contrôle les chunks ont une taille variable. Les principaux chunks définis dans SCTP sont récapitulé dans la table suivante :

ID valeur	Chunk type	DESCRIPTION
0	Données DATA	Les données d'utilisateur
1	INIT	Initiation d'une association
2	INIT ACK	Acquittement de la portion INIT
3	SACK	Acquittement de la réception de données
4	HEARTBEAT	Vérifier l'accessibilité via des chemins alternatifs
5	HEARTBEAT-ACK	Acquittement de la portion HEARTBEAT
6	ABORT	Fermeture immédiate d'une association
7	SHUTDOWN	Début de la fermeture normale d'une association
8	(SHUTDOWN ACK	Acquittement de la portion SHUTDOWN
10	COOKIE ECHO	Porte le COOKIE pendant l'initialisation d'une association
11	COOKIE ACK	Acquittement de la portion COOKIE ECHO

Figure 4.10 : listes des types des chunks, selon RFC2960

- **HEARTBEAT** : pendant l'établissement d'une association, les chunk INIT, INIT-ACK peut portent d'autre adresses lorsqu'il s'agit d'un hôte multi-homed, SCTP défini un mécanisme utilisé par un hôte réseau pour confirmer l'accès a ces adresses, ce chunk est envoyé cycliquement (toutes les 30s) Les requêtes HERARTBEAT doit acquittées par des HEARTBEAT-ACK

- **Accusé sélectif (SACK) :** ce chunk pour acquitter des données reçu, ou bien d'informer l'émetteur d'éventuels "gaps" ou absence dans certains chunks DATA, il utilise une liste des paramètres
  - *Cumulative TSN Ack :* ce paramètre contiens le TSN du dernier DATA chunk reçu dans une séquence avant une gap.
  - *Gap Ack Block Start* : indique le début du GAP
  - *Gap Ack Block End* : *indique la fin du GAP*

- **COOKIE ECHO** *:* ce chunk est utilise seulement dans la phase d'initialisation d'une association, il est envoyé par l'initiateur pour compléter le processus d'établissement .ce chunk **DOIT** précède tout transfert de données, mais peut contenir des chunks de données dans le même paquet.

- **COOKIE ACK :** utilise pour informer l'autre point de la bonne réception du cookie, comme le précèdent, ce chunk doit précède tout transfert des données mais peut contenir des données dans le même paquet

7.8 Échange des données :

Comme SCTP hérite les avantages de TCP (fiabilité, contrôle de congestion, ….), le mode de connexion implémenté dans la spécification du SCTP, est similaire au TCP, avant toutes échange des données, les deux entités doivent établie une association entre eux, cette association SCTP passe par les états "établissement", "échange " puis "fermé".

7.8.1 Établissement d'une association :

Chaque association SCTP entre deux hôtes est initialisée par quatre paquets (TCP utilise trois paquets) la bonne nouvelle du SCTP est que les données peuvent être inclus dans le 3éme et le 4éme message [2], ceci peut minimiser le délai tout en augmentant la sécurité. Le premier, un bloc INIT, est envoyé, en réponse il reçoit un paquet INIT ACK contenant un témoin (cookie), ensuite la connexion peut démarrer en envoyant les données. Cependant, deux paquets supplémentaires sont envoyés. Le témoin reçoit en réponse un bloc COOKIE ECHO, lequel reçoit enfin un bloc COOKIE ACK.

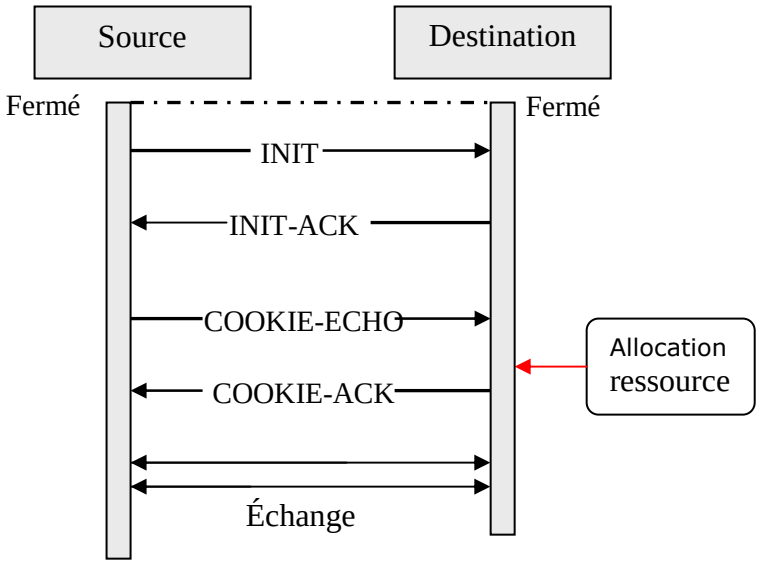


Figure 4.10 Scénario d'ouverture d'une association SCTP

Afin de surmonter aux problèmes existe dans le protocole TCP, tel que les *attacks* SYN (dans ce type d'attaque, l'attaquant inonder le victime par un nombre important de requêtes de connexion de type SYN (équivalent à INIT dans le SCTP), le système cible réserve des ressources (espace mémoire) pour chaque requête reçu, jusqu' à il ne peut servir aucune demande. Ce 'est le DoS (Denial of Service), SCTP résout ce problème par l'établissement de l'association en quatre temps, et ne réserve aucun espace mémoire qu'après le client initier son cookies avec COOKIE-ECO (voir le figure 4.10.)

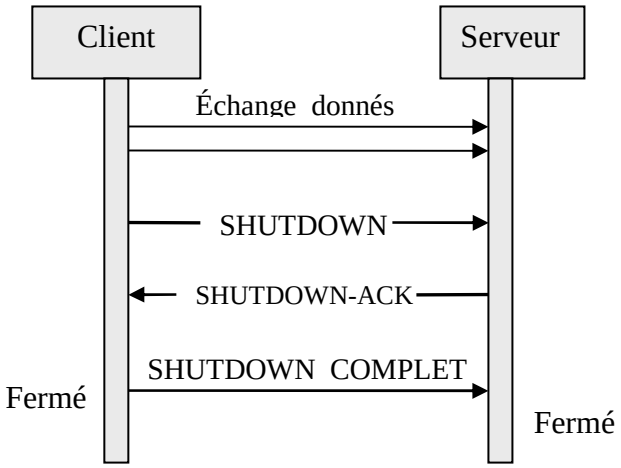
7.8.2 Envoi de données et contrôle de session :

SCTP, à ce niveau, l'échange des données peuvent mis en place, dans SCTP il existe des blocs de contrôle et des blocs de données, comme nous avons vu, les blocs de données sont envoyés en utilisant le bloc DATA, auquel il est répondu par un bloc SACK, ça fonctionne pratiquement de la même façon que TCP SACK. Les blocs SACK sont des blocs de contrôle.

Au dessus de tout ça, il existe d'autres blocs de contrôle. Les blocs HEARTBEAT et HEARTBEAT ACK d'un côté, et les blocs ERROR de l'autre. Les blocs ERROR sont utilisés pour informer des divers problèmes ou erreurs de connexion, comme un *ID* de flux invalide ou des paramètres de données obligatoires absents, etc.

7.8.3 Fermeture d'une association :

Tout protocole de communication fiable nécessite une méthode pour terminer une communication, la procédure de fermeture d'une association dans SCTP peut être initiée par les deux cotés d'une association en utilisant trois messages comme montré sur la figure 4.11 et décrit ci-dessous.



4.11 Scénario de fermeture d'une association SCTP

1. L'émetteur envoie un message SHUTDOWN au récepteur, qui indique que le client est prêt à fermer la connexion.
2. Le récepteur répond en envoyant un message de SHUTDOWN-ACK.
3. L'émetteur envoie alors un message de SHUTDOWN-COMPLETE en retour au récepteur.

7.9 Etablissement d'une association entre les protocoles SCTP et AODV :

SCTP établit l'association par les 4 messages (INIT, INIT-ACK, COOKIE-ECHO et COOKIE-ACK), AODV utilise 2 messages (Route Request et Route Reply).

La Figure ci-dessous illustre le mécanisme de création d'une association SCTP avec création de routes AODV. On suppose que la route n'est plus existe dans table cache du AODV

1. le SCTP initié une association par l'envoie d'un message INIT.
2. AODV mémorise le paquet SCTP. pour créer un chemin entre les deux nœuds, il lance une requet de découvert de route Route_request, et attendre une réponse Route_Reply
3. Quand AODV peut utiliser la route vers le noeud destination, SCTP poursuit l'établissement d'association. INIT est transmis par le niveau routage,
4. le noeud destination répond, il envoie un INIT-ACK. La source reçoit en réponse un COOKIE-ECHO, le quel reçoit enfin un COOKIE-ACK;
5. L'émission des données peut commencer

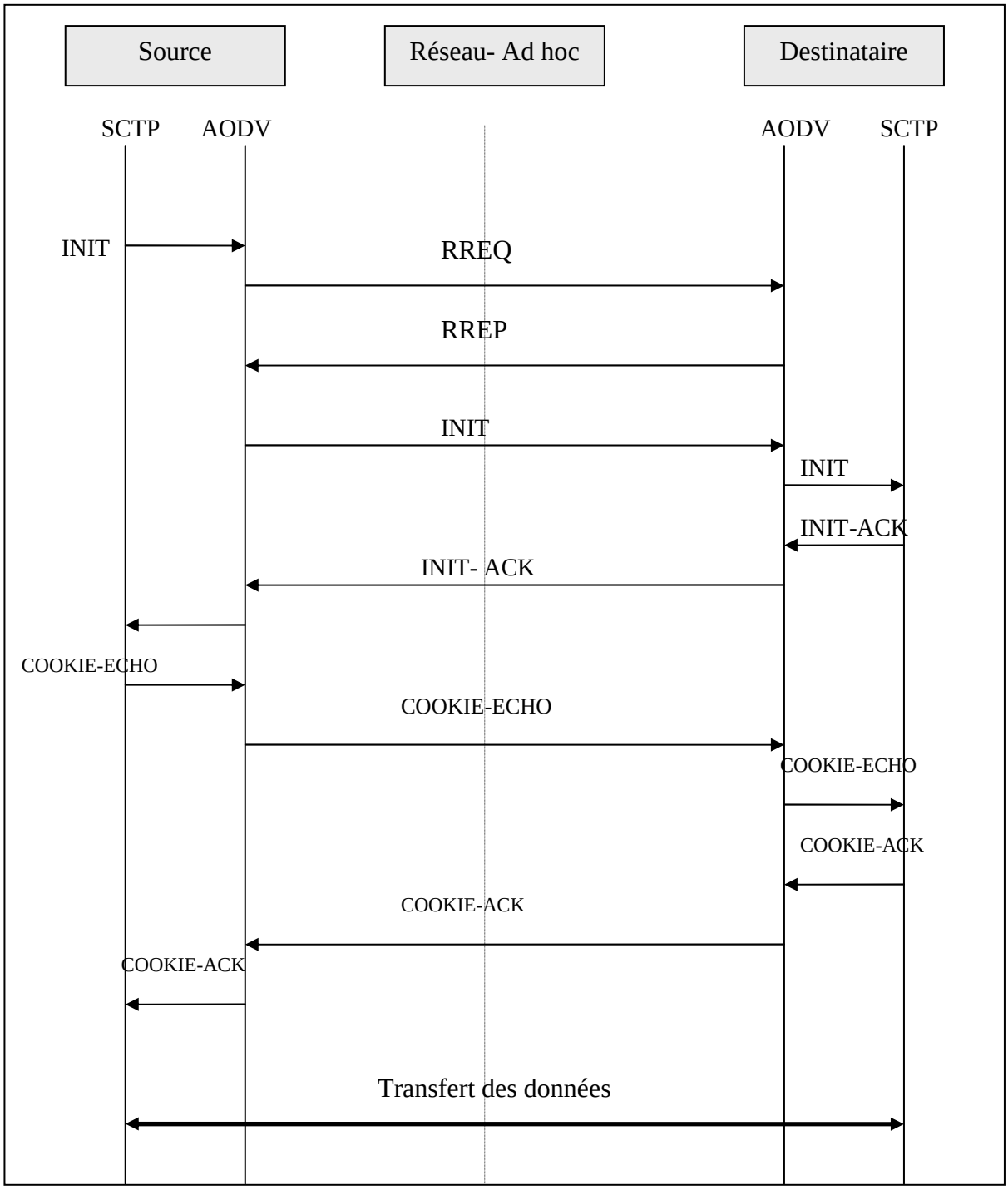


Figure 4.12 : Diagramme Interaction entre les deux protocoles SCTP et AODV

8. Contrôle de flux et congestion :

La congestion est un phénomène d'accumulation des paquets dans certains nœuds du réseau, qui traduit leur surcharge et leur difficulté à écouler un trafic devenu trop important. Le ralentissement ou la perte de paquets qui en résultent peuvent conduire l'émetteur qui ne reçoit plus les acquittements de ses paquets dans les délais de temps impartis, à les réémettre, augmentant par là même un trafic déjà saturé.

Le phénomène de congestion, s'il n'est pas contrôlé efficacement, peut, comme on le voit, conduire à l'effondrement du réseau. Lorsqu'une congestion survient, SCTP réagit en réduisant le débit de la connexion.

Les mécanismes définie dans SCTP sont globalement équivalents à celles-ci utilisées dans TCP tel que les variables cwnd, rwnd et ssthresh ou les mécanismes slow-start et congestion avoidance, SCTP introduit une variable supplémentaire *pba* "Partial_bytes_acked" qui calcule l'augmentation de *cwnd* pendant la phase d'évitement de congestion, de même que TCP, SCTP souffre du problème du réseau sans fils de la mauvaise interprétation du perte des paquets

SCTP effectue le slow-start lorsque $cwnd \leq ssthresh$, et l'évitement de congestion lorsque $cwnd > ssthresh$, d'augmenté le cwnd par 1MTU chaque RTT, SCTP utilise *pba* pour facilite cet mécanisme [11] pour la détection des pertes SCTP utilise deux mécanismes le Fast Retransmit ou Retransmission timeout

Le document RFC [4460], élaboré par l'IETF pour le traitement de la congestion le deuxième document une compilation de tous les défauts existent dans viennent de corriger les défauts du premier version, les principales valeurs de CWND sont résumés dans cette table

	Ancienne valeur	Nouvelle valeur
La valeur initiale de CWND avant une transmission ou longue période d'inactivité	2*MTU	Min (4*MTU, Max (2*MTU, 4380 bytes))
S'il y a des pertes par SACK	$ssthresh = \max(\frac{CWND}{2}, 2*MTU)$ $CWND = ssthresh$	$ssthresh = \max(\frac{CWND}{2}, 4*MTU)$ $CWND = ssthresh$
Expiration T3-rtx, SCTP effectue SS	$ssthresh = Max(\frac{CWND}{2}, 2*MTU)$ $CWND = 1*MTU$	$ssthresh = \max(\frac{CWND}{2}, 4*MTU)$ $CWND = 1*MTU$

Accusés sélectifs (SACK) :

Les acquittements porte toutes les numéros TSN été reçu de façon intact, cet caractéristique devienne obligatoire avec SCTP, il y aussi ce qu'on appelle **Gap blocks** qui indique l'absence d'un certains segments situent entre d'autres segment qui sont bien reçu

9. Le Multistreaming :

La possibilité d'avoir plusieurs streams indépendants dans une association est une caractéristique qui rend SCTP différents des protocoles de transport existant, Contrairement au TCP où les données sont transmis en flot d'octet, les données dans SCTP sont transmis en flot de messages, en plus, SCTP permet d'avoir plusieurs stream de données multiplexés dans une association, où chaque stream dote d'un identificateur *ID_stream*, pour distinguer d'autre stream, le nombre de stream (entrant /sortant) dans une association est négocie pendant la

phase d'initialisation grâce paramètres NOS "Number of Outbound Stream" NIS "Number Inbound Stream" dans le chunk INIT, de l'autre coté le récepteur réserve un buffer pour chaque stream.

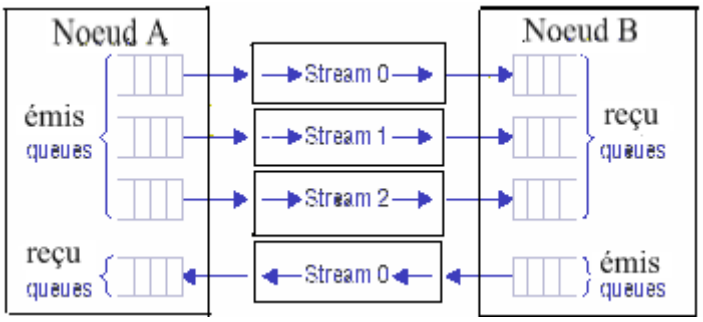


Figure 4.13 le concept de multistreaming

Par cette propriété SCTP crée une indépendance entre la transmission et la délivrance des données. Qui permet de casser la forte restriction de délivrance par ordre existe TCP, qui souvent résulte le problème HOL "Head Of Line" existe dans les connexions TCP. Dans SCTP si un message est bloqué ou retardé dans un stream ceci n'affecte que le stream concerné, les autres puissent être délivrés au destinataire figure 13.

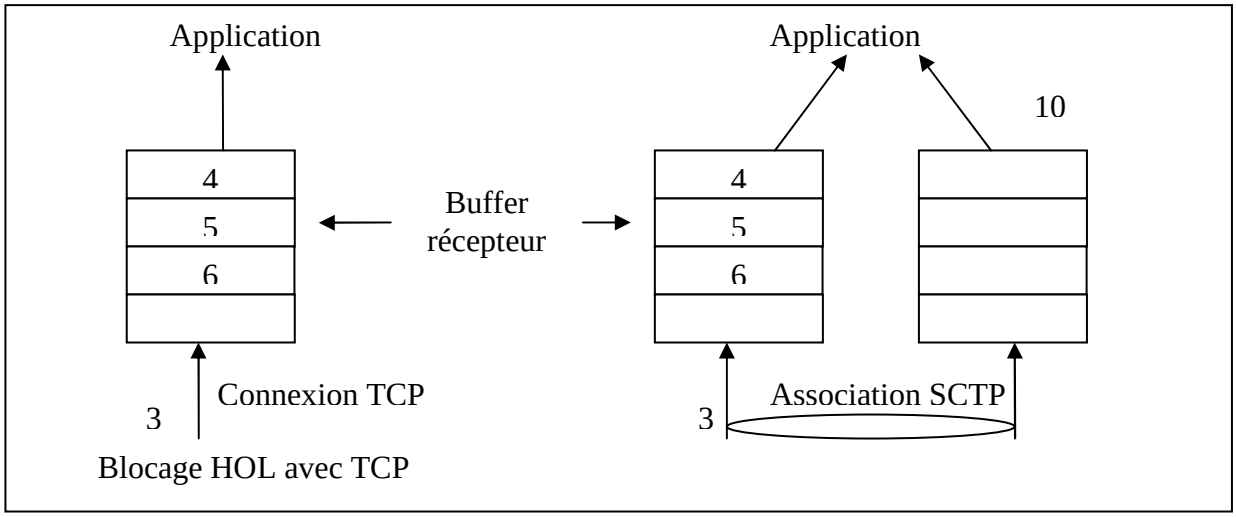


Figure 4.14 : La résolution du problème HOL à l'aide du Multistreaming

Plusieurs applications peuvent bénéficier de cette propriété, notamment les protocoles de signalisation et les navigateur web [14].dans le premier cas, ce qui est essentiel c'est l'indépendance des flots dans une association et la possibilité de livraison de messages dans le deuxième cas, le navigateur peut télécharger une page entière dans une association .tous les objet de la page peuvent être téléchargé en même temps dans des flots indépendant .cela permet d'économiser des ressources, du coté de client aussi bien de que du coté du serveur

10. Le Multihoming

Le Multihoming ou la multidomiciliation se reporter à la situation où un réseau ou un hôte est accessible via plusieurs interfaces réseau figure 4.13., La première idée de Multi-homing est de créer des connexions redondantes à l'Internet à travers différents ISPs (ou un seul ISP avec plusieurs connexions Internet) c'est une solution procure par les organismes pour

améliorer l'accessibilité et la prise en charge du public aux leurs sites web [1] ici on parle d'un ˝site Multihoming. L'autre idée du Multihoming c'est l'augmentation de la robustesse du réseau, par un basculement du flux d'information d'un chemin en panne vers un chemin en fonctionnement, ou pour la retransmission des données perdues, la répartition de la charge sur plusieurs chemins est un sujet au cours de la recherche dans la communauté scientifique.

Figure 4.15 Principe du Multihoming

10.1 Le Multi homing dans les réseaux ad hoc :

Dans un réseau ad hoc un nœud multihomed est un nœud possède plus d'une interface réseau. Dans notre étude l'intérêt majeur du Multihoming auquel nous intéresser dans ce mémoire : est de crée un niveau de redondance par l'établissement de plusieurs chemins entre les points terminaux, l'un est considéré comme un chemin primaire et les autres sont redondants, cela permet d'augmenter la tolérance aux défauts de la route et une rapidité de recalcule des chemins e diminue partiellement le problème de la rupture fréquente des chemins. Ceci on créant un chemin primaire et d'autres alternatifs pour des retransmissions [3]. au niveau transport le protocole TCP ne supporte pas des équipements multicartes, par contre SCTP ayant la faculté de gérer ce type d'hôtes cette propriété distingue le SCTP aux autres protocoles de transport.

10.1.1 La Gestion des adresses lors de la phase d'initialisation :

Si le client est multi-homed, celles-ci peuvent être utilisées dans une association SCTP. Le client informe le serveur de l'ensemble de ses adresses IP lors d'initialisation dans le chunk INIT, par contre le client doit connaître une seul adresse IP du serveur puisque les autres adresses sont renvoyées automatiquement dans le chunk INIT-ACK, une instance SCTP considère chaque adresse IP de l'autre point terminal comme un chemin distinct

10.1.2 Contrôle des chemins redondants avec SCTP :

Lorsque l'association SCTP est établi entre deux nœuds multihomed, une instance SCTP doit contrôler tous les chemins inoccupés appartient à l'association, a cet effet un chunk HEARTBEAT envoyé périodiquement vers tous les interfaces hôte correspondant, et chaque HEARTBEAT doit acquitter par un paquet HEARTBEAT-ACK, et pour chaque chemin SCTP attribue une variable pour contrôle d'état active ou inactive, si après plusieurs tentative le client ne reçoit pas des accusées l'interface redondante est considéré comme inaccessible.

11. Comparaison des performances de TCP et SCTP dans les MANETs:

Apres une description de ces deux protocoles, nous essayons d'étudier leurs performances lorsqu'il s'agit d'un réseau ad hoc. Dans l'article [12], [13] les performances de TCP dans les réseaux ad hoc apparaissent meilleures que celles de SCTP en terme de goodput, cette est montré dans la figure 4.11. Les auteurs rendent cette principalement, d'une option SACK dans le SCTP qui occupe une large bande passante, cependant l'analyse des résultats de la simulation dans ces deux articles est très gourmande.

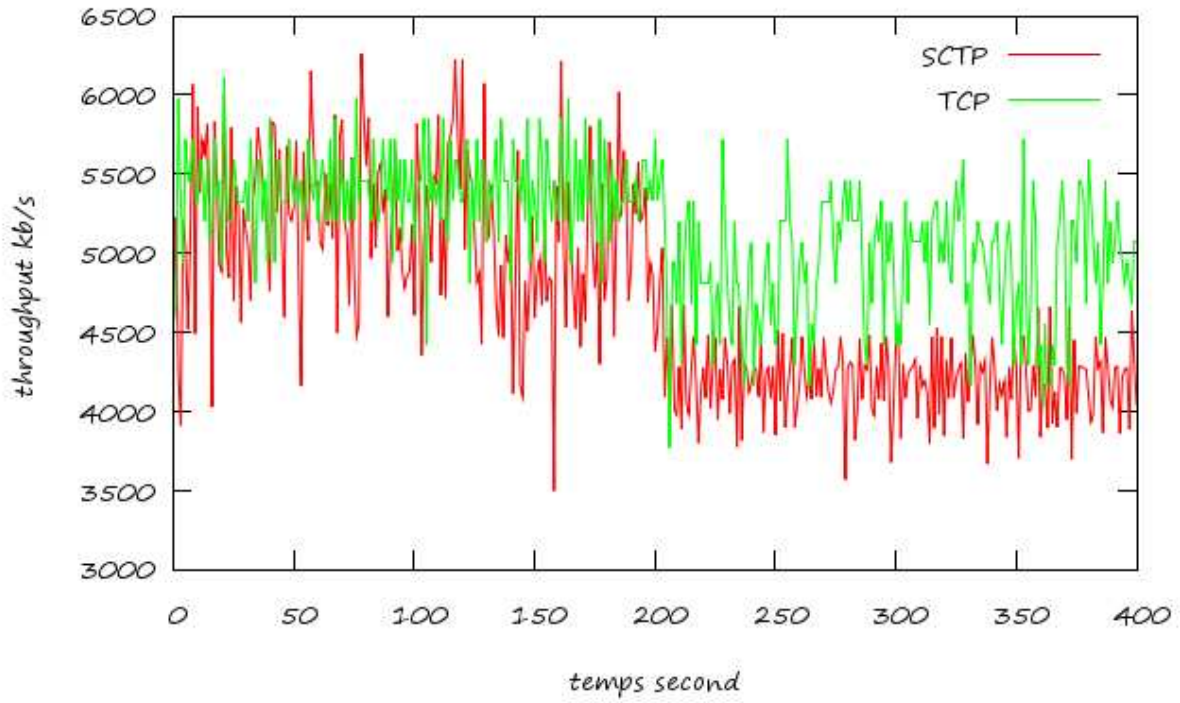


Figure 4.16 Comparaison entre TCP et SCTP avec un nombre de Streams égale à 4

Pour mieux exploiter les caractéristiques du SCTP nous essayons de modifier des paramètres environnementaux “taux d’erreur” ou les caractéristiques lier au comportement du protocole SCTP “la taille des buffers. La table suivante résume les différents paramètres de la simulation.

Les différents résultats sont montrés dans les figures qui suite :

Nombre de nœuds	9
Type de trafic	FTP
Surface du terrain de la simulation	800m x 800m
Vitesse de mobilité	[0 : 5] m/s
Nombre de Streams par association	4 Stream
Taux d’erreur	10^{-6}

La figure 4.11 montre le gain de performance entre deux nœuds, selon les paramètres décrits :

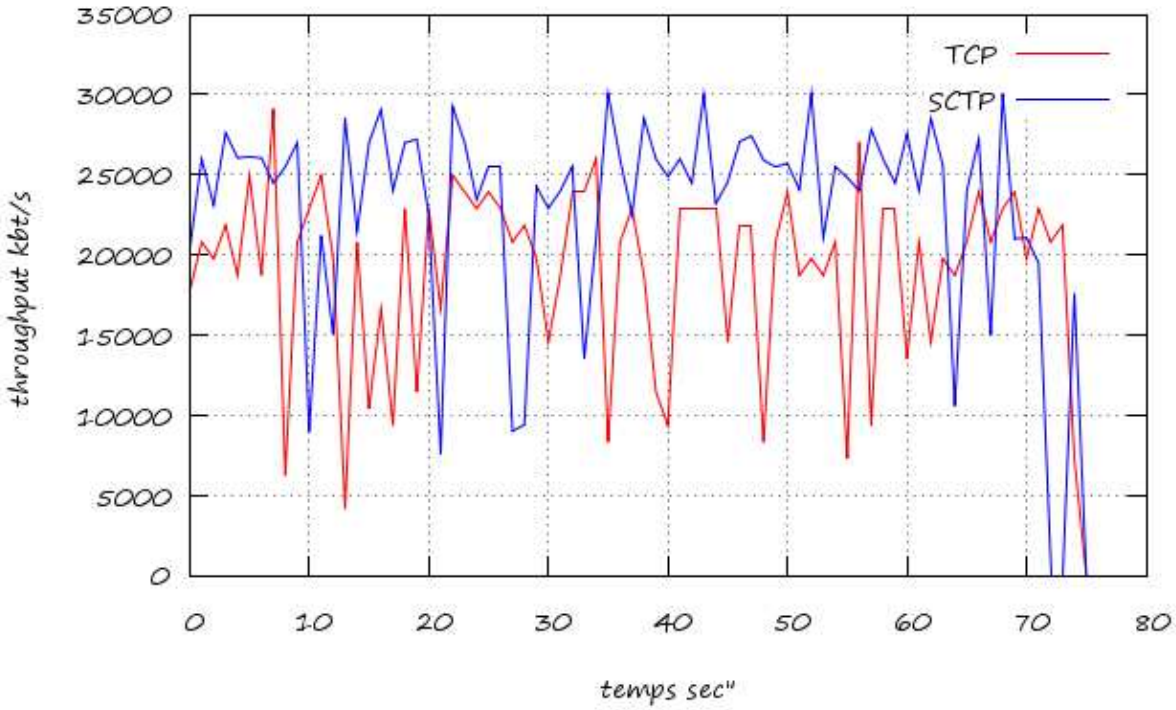


Figure 4.17 : TCP et SCTP dans un réseau ad hoc

Nous avons remarqué que le throughput cas du protocole SCTP est plus élevé que dans le cas du TCP, est plus robuste dans des environnements bruité, cela revient à la capacité de correction d'erreur dans SCTP car il utilise un code correcteur de 32 bit, contre 16 bits dans le TCP, ainsi l'effet de multistreaming qui prouve ces efficacité dans environnements bruité

8.1 Effet de nombre de stream sur le rapport de livraison des paquets :

Dans cette simulation nous montrons l'effet de la taille des buffers au niveau du récepteur, sur le taux des paquets délivrés PDF "Packet Delivery Fraction ", nombre de stream sur

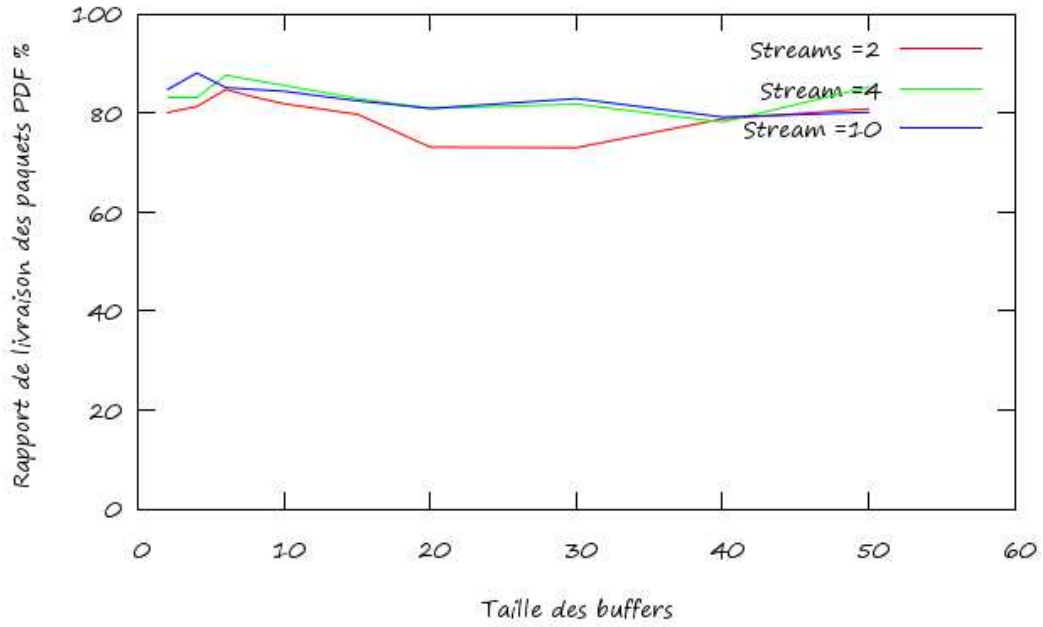


Figure 4.18 : Rapport de livraison des paquets selon la taille des buffers

Pour le nombre de stream égale à 2
Car le entête d'un stream peut générer une surcharge sur le réseau et une

8.2 Effet du Multihoming :

Pour voir les performances du multihoming, dans un réseau ad hoc nous avons défini les deux scénarios suivants :

a) : tous les nœuds sont Mono-homed
b) : tous les nœuds sont Multi-homed

Les différents paramètres du SCTP sont récapitulés dans la table suivante :

Type de Trafic	CBR
Transport	SCTP
Nombre de Streams par association	2
Protocole de routage	AODV
Mobilité	Faible

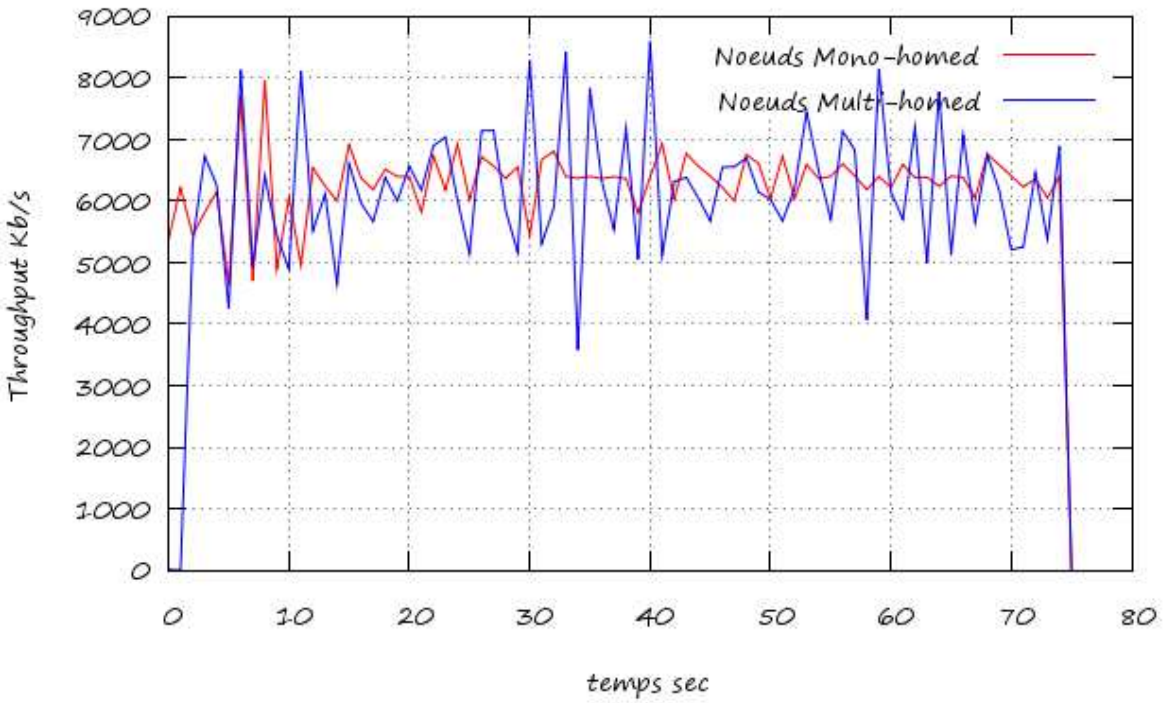


Figure 4.19 : le débit moyen

D'après les résultats de la simulation nous remarquons, dans le cas (b) où le réseau est constitue par des noeuds Multi-homed est plus performant que dans le cas (a), cela est du de l'effet du chemin secondaire car les acquittements et les retransmissions se faire sur ce chemin, ce qui diminue la charge sur le chemin primaire et augmente le débit de transmission. L'inconvénient de cette technique réside dans le temps nécessaire pour commencer le transfert, car chaque nœud doit annoncer ces différentes adresses IP disponibles pendant la phase d'établissement de l'association, de l'autre coté chaque nœud participe dans l'association vérifie la validation des chemins vers ces adresses IP par des messages "HEARTBEAT"

12. Problème d'intégration Multihoming/multichemin pour les réseaux ad hoc :

Les protocoles multichemins améliorent la robustesse des routes dans les réseaux mono-domiciliés, cependant, leurs déploiements dans des réseaux ad hoc multi-domiciliés nécessitent des modifications pour qu'ils prennent en charge le Multihoming des nœuds. Afin de créer des routes disjointes en nœuds entre les nœuds extrémités multi-homed, les auteurs dans l'article [23] décrit une méthode spécifique de découverte des routes, quand un nœud destinataire multi domiciliés reçoit un paquet RREQ, il répond par un RREP qui inclut la liste de ses adresses IP disponibles (figure 4.), l'émetteur exécute une fonction ADDIP, qui permet la mis à jour de la liste des adresses de l'association SCTP, puis lance un nouveau processus de découverte RREQ_IP_2 vers l'adresse IP_2. Les nœuds intermédiaires qui fait l'ensemble du premier chemin, ne route pas le paquet RREQ_IP_2.

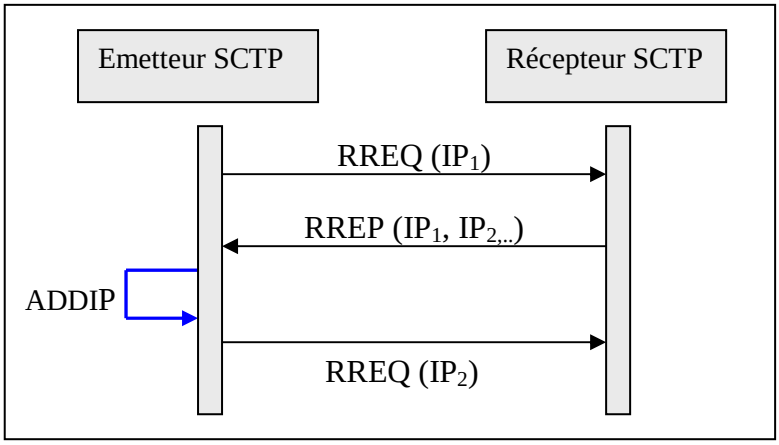


Figure 4.20 Diagramme de séquence découverte de la route pour des nœuds Multihoming

Vers l'adaptation par une cross layer :

Les auteurs dans l'article [24], [25] exposent une autre problématique de l'intégration Multihoming / Multipath dans les réseaux ad hoc, la topologie proposé est constituent des noeuds Multihomed et définis AODV comme un protocole de routage. Les différent cas sont définis comme suite :

a) Deux chemins de transport avec un nœud intermédiaire commun figure (a)

Chemin primaire : IP1→ IP3 → IP7
Chemin alternatif : IP1→ IP4 → IP8

b) Un chemin avec deux chemins disjoints en nœud figure (b)

Chemin primaire : IP1→ IP3 → IP7
Chemin redondant : IP1→ IP5 → IP8

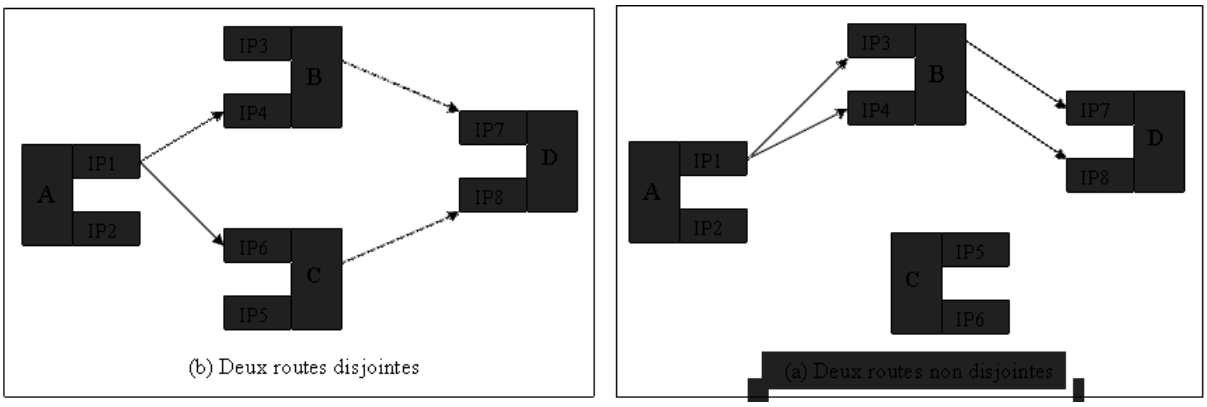


Figure 4.21 : différentes topologie d'intégration du multihoming / multichemin

Pendant la simulation deux problèmes apparaissent :

1. **Problème "discontinuité du transfert de données " :**

   Lorsqu'il y a une rupture dans la route, le nœud source ne peut continue le transfert sur le chemin alternatif, car il ne sait pas que cette route arrive à la même destination, ainsi comme l'adresse destinataire du chemin alternatif diffère de celle du chemin primaire. AODV ne l'utilise pas mais il relance un nouveau processus de découverte de la route.

2. **Problème "requête de route superflue"**

Quand un nœud intermédiaire retourne un paquet RERR, le nœud source relance deux requêtes RREQ, l'une pour rétablir le chemin primaire (vers la première carte), l'autre pour la route alternative, même si cette route était encore existe, l'autre exemple de requête superflue est en cas d'arrivé d'un RREQ le noeud le diffuse trois fois.

Les auteurs rend ces phénomène inattendu à une lacune entre le niveau réseau et transport résulte un manque d'échange d'information entre les deux niveau, AODV travaille au niveau nœud sans considérer les interfaces, ainsi un nœud de transport multi-homed est vu comme un groupe de nœuds, il est composé d'un nœud central (core node), tel que le nœud A, et de plusieurs nœuds "interfaces" tels qu'IP1 et IP2, donc un nœud avec N interfaces est considéré comme Nœud, et le nœud central dans l'opération de routage agit comme un noeud d'interface

Afin d'accélérer la reprise du routage les auteurs proposent une solution consiste d'insérer d'une cross layer entre les niveaux 3 et 4, celle-ci permet aux couches transport et réseau d'échangent d'information et d'adapter dynamiquement aux changements de la topologie du réseau une vue globale cette CLI est répartie sur tous les nœuds du réseau, et d'échange des informations

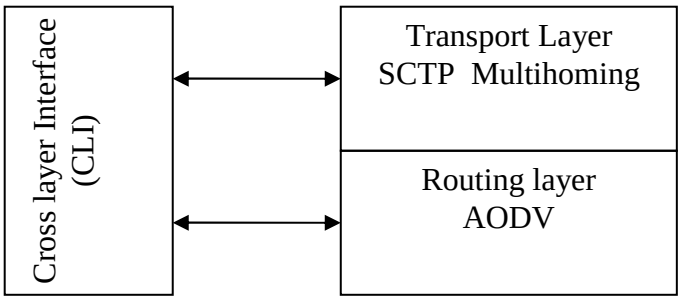


Figure 4.22 : inter couche CLI

Solution

Les auteurs dans l'article [24] proposent d'insérer une cross layer entre les deux niveaux afin de permet une commutation systématique vers un chemin secondaire quand le premier chemin devient invalide, mais la solution proposé consiste plus d'insère d'autre fonction au protocoles AODV Pause, la fonction Change_Path qui permet au protocole AODV de réagir avec les changement de la route sans interrompre la connexion. Dans le chapitre suivant en essaye de proposé notre propre architecture qui est basé sur une cross layer, avec des nouveaux concepts et philosophie des réseaux.

13. Conclusion :

L'une des solutions qui augmente la robustesse des routes dans les réseaux ad hoc est le routage par chemins multiple comme on a déjà voir dans le deuxième chapitre, cette solution est efficace d'un coté de diminution le temps de rétablir des route, mais d'un autre coté elle est peu limité car elle génère des complexités au niveau transport si elle utilise plusieurs chemin à la fois, une autre approche consiste à équiper un nœud par plusieurs interfaces, où chaque carte peuvent établir un chemin distinct vers le destinataire, ici on parle d'une combinaison d'un routage multichemin avec un multihoming, cependant le protocole de transport TCP ne supporte pas cette l'idée de multi-cartes, car dans son conception initial il peut gère qu'une seul carte à la fois.

SCTP le nouveau protocole de transport, hérite des caractéristiques de TCP, ainsi il porte des nouveaux concepts propre tel que le multistreaming et le multihoming, ces caractéristiques peuvent augmenter les performances d'un réseau ad hoc, notamment le problème du ruptures des chemins, l'idée d'augmenter la robustesse des route par de multihoming mais ils y a des problèmes se posent, l'un de ces problèmes quand il y a une échec dans la route, tel que la discontinuité du transfert et les requêtes superflue, de la mauvaise communication entre les deux protocoles AODV et SCTP, une solution proposé à ce problème consiste d'insérer une cross layer entre les niveaux transport et réseau, cette cross layer est répartie sur tous les nœuds du réseau.

Référence :

[1] W. Stallings “Data and Computer communication” PRINTICE HALL 8 éme edition

[2] R. Stewart, Q. Xie “Stream Control Transmission Protocol” RFC 2960, IETF, Octobre 2000

[3] L. Ong “An Introduction to the Stream Control Transmission Protocol (SCTP)” RFC 3286 IETF, may 2002

[4] R. Stewart RFC [4460] “Stream Control Transmission Protocol (SCTP) Specification Errata and Issues” 2006.

[5] O. Bazan,U. Qureshi, M. Jaseemuddin “Performance evaluation of TCP in Mobile ad-hoc networks” The Second International Conference on Innovations in Information Technology (IIT’05)

[6] A. Al Hanbali, E. Altman, P. Nain, “A Survey of TCP over Mobile Ad Hoc Networks”, rapport de recherché no. 5182, INRIA Sophia Antipolis research unit, Mai 2004 .

[2] J. Postel “Transmission control Protocol” RFC 793 IETF September 1981

[3] S.K Sarkar, T.G basavaraju “Ad hoc mobile principles, protocols, and application” Auerbach publication 2007

[4] Z.Fu,P.Zerfos,H Luo,S Lu,L Zhang, M Gerla “The Impact of Multihop Wireless Channel on TCP Throughput and Loss” IEEE INFOCOM 2003

[7] J.Liuand S.Singh, “ATCP: TCP for mobile ad hoc networks”, IEEE Journal Selected Areas in Communications, vol.19, pp.1300-1315, Juillet 2001

[8] D.Kim, C.K Toh et Y. Choi, “TCP-Bus: Improving TCP Performance in Wireless Ad-Hoc Networks”, Journal of communications and networks, vol.3, no.2, Juin 2001.

[9] S. Kopparty, S. Krishnamurthy, M. Faloutous, and S. Tripathi, “Split TCP for mobile ad hoc networks”, in Proc. of IEEE GLOBECOM, Taipei, Taiwan, Nov. 2002.

[10] F. Wang and Y. Zhang, “Improving TCP performance over mobile ad hoc networks with out-of-order detection and response”, in Proc. of ACM MOBIHOC, Lausanne, Swisse, pp. 217-225, Juin. 2002

[11] Z. Fu et B. Greenstein, “Design and Implementation of a TCP-Friendly Transport Protocol for Ad Hoc Wireless Networks”, IEEE International Conference on Network Protocols (ICNP'02), pages 216-228, Paris, France, Nov. 2002.

[12] W. Stevens “TCP/IP illustrated Vol1” edition Addison –Wesley 1995

[13] Shiduan Cheng, Jian Ma, and Fei Peng, “A proposal to apply ECN to wireless and mobile networks”, Internet Society INET (2000)

[14] R.Stewart, C.Metz “SCTP : New Transport protocole” journal IEEE 2001

[15] A. L. Caro and al “SCTP: A Proposed Standard for Robust Internet Data Transport” journal IEEE 2003 pp 56-63

[16] F Buntchu R.Scheure , A. Delly “une Alternative à TCP et UDP” novembre 2003

[18] F. Buntschu, R. Scheurer and A. Delley“SCTP (Stream Control Transmission Protocol) Une alternative à TCP et UDP?”

[19] Armando L. Caro Jr., Keyur Shah, Janardhan R. Iyengar, Paul D. Amer "SCTP and TCP Variants: Congestion Control Under Multiple Losses"

[20] A. Kumar and L. Jacob,"SCTP vs TCP : Performance Comparison in MANETs", Proceedings of the 29 th Annual IEEE International Conference on Local Computer Networks (LCN),2004.

[21] A. Argyriou and V. Madisetti "Performance Evaluation and optimisation of SCTP in Wireless ad hoc Networks" procedding of the 28th Annual IEEE international Conference on Local Computer Networks (LCN'03) 2003

[22] http:// www.iec.org International Engineering Consortium "Stream Control Transmission Protocol"

[23] Ki-Il Kim "A Cross Layered Approach for Multihoming on SCTP in Mobile Ad Hoc Networks" journal IEEE 2007.

[24] S. Charoenpanyasak and B. Paillassa "SCTP multihoming with Cross Layer Interface in Ad Hoc Multihomed Networks" third IEEE International Conference on wireless and mobile computing 2007

[25] S. Charoenpanyasak "Optimisation inter-couches du protocole SCTP en réseaux ad hoc" these doctorarat juin 2008

Chapitre 5 :

Optimisation par cross layer

1. Introduction :

La solution que nous allons proposer, consiste d'insérer une cross-layer entre la couche réseau et transport, cette solution est inspirée de l'architecture HIP "Host Identifier Protocol" [1], qui se base sur le principe de découpler la dépendance entre ces deux couches. L'idée d'optimisation par une "cross layer " dans les réseaux ad hoc n'est pas nouvelle. MAN "Mobile Métropolitain ad hoc Network" [2] est un exemple d'optimisation par une cross layer. Dans cette architecture les différentes couches de la pile TCP/IP sont capables de communiquer entre eux même si ces couches ne sont pas forcément adjacentes, ce qui permet une bonne interopérabilité entres ces différentes couches. MAN s'appuie sur un composant central qui est le "Network Status" figure 5.1, où chaque protocole peut accéder à cette entitée pour partager ses données avec les autres protocoles. Cette architecture modifie le principe du TCP/IP où le seul moyen d'échange des données de contrôle s'effectue entre les couches adjacentes.

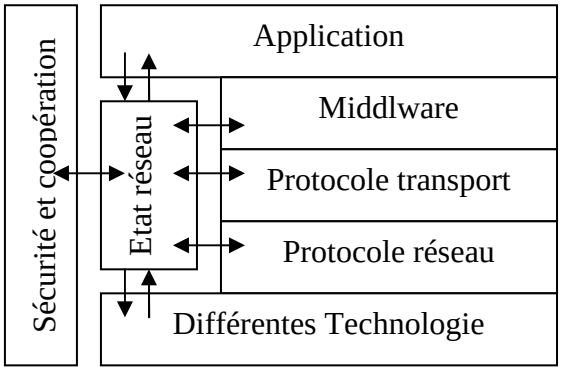


Figure 5.1 : L'architecture MAN

L'article [3] montre aussi de nombreuses solutions basées sur une optimisation par cross layer, chaque solution traite un problème spécifique dans les réseaux ad hoc, ainsi beaucoup de ces problèmes est du à la mauvaise implémentation de l'architecture actuelle TCP/IP dans les réseaux sans fil, car initialement celle-ci a été conçu pour des réseaux filaires caractérisés par un environnement stationnaire et une absence de mobilité.

2. L'architecture HIP "Host Identifier Protocol" :

Dans l'architecture TCP/IP actuelle, pendant l'opération d'échange une adresse IP joue une double fonction, elle joue le rôle d'un identificateur d'un hôte et d'un localisateur pour le routage, c'est-à-dire que l'identifiant et le localisateur d'un hôte sont confondus dans une seul adresse IP, ainsi les applications Internet identifient un hôte par le couple « adresse IP, numéro de port ». HIP "Host identifier Protocol" décrit dans les documents [1], [4], [5], [6] est une solution proposée face aux problèmes rencontrés dans les réseaux sans fil tel que l'adressage dynamique des nœuds cas du mobile IP [7], ou le roaming d'un nœud ente différent réseaux ou le Multihoming lorsqu'il s'agit d'un réseau multi-accès. Tout ces cas implicite un changement d'adresse, ce qui nécessite un mécanisme de gestion des adresses IP, toute sans la perte de connexion. (Cas du Mobile IP)

Le nombre des documents RFC publié par IETF sur cette architecture (8 RFC), montre que le protocole HIP est une solution intéressé par les chercheurs de la communauté Internet, et peut prendre sa place dans l'architecture Internet, car il peut résoudre de nombreux problèmes existent dans l'architecture actuelle.

Implémente l'architecture HIP tel qu'elle est dans les réseaux ad hoc, demande un effort de plus, car elle base sur des notions de la cryptographie, des algorithmes de chiffrement Diffi-Helman et sur des entités centralisé tel le DNS "Domaine Name System". La solution que nous proposons repose sur le principe de base HIP qui est le découplage entre les deux niveaux transport et réseau et l'insertion d'un nouvel identificateur autre que l'adresse IP, et limiter le rôle de l'adresse IP seulement au routage.

3. HIP et la couche transport

Une connexion TCP/IP est identifié par le quadruplet «adresse source ; numéro de port ; adresse destinataire ; numéro de port», si l'un de ces paramètres change, la connexion doit rétablir, ce schéma rend les protocoles de la couche transport (TCP, UDP, SCTP) dépendent de l'adresse IP, qu'est une composante de la couche réseau, et elles peuvent varier dans le temps. Le but du protocole HIP est de découpler cette dépendance et rendre l'évolutions de chaque couche indépendante l'une de l'autre en spécifiant que l'adresse IP reste comme un localisateur utilisé pour les opérations du routage, et le HI *"host Identifier"* comme un identifiant du hôte, de cette façon une connexion sera identifie par « HI source ; Numéro de port ; HI destinataire ; Numéro de port », si il y a un changement d'adresse IP, cela n'influe pas sur la connexion et elle reste ouverte figure 5.2

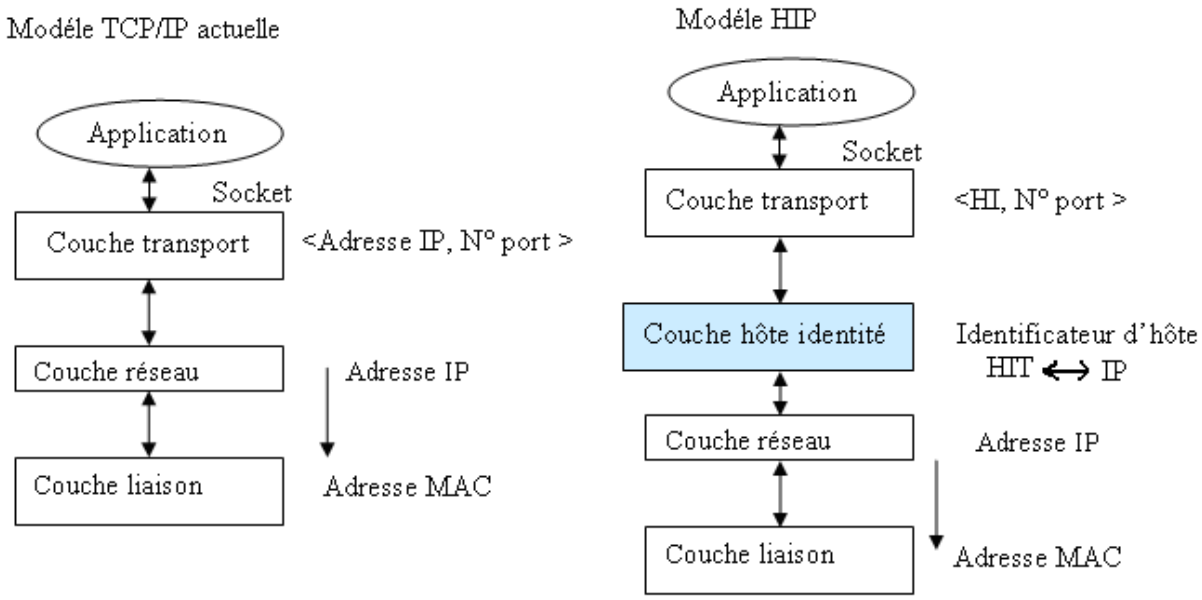


Figure 5.2 : *Comparaison entre l'Architecture actuelle da la pile TCP/IP et architecture HIP*

La définition du HI comme un identifiant unique, permet aux protocoles de la couche transport TCP, SCTP de remplacer les adresses IP par ce HI dans les paquets, afin de conserver la compatibilité avec l'architecture standard, nous définissons la longueur du HI sur 128 bits.

4. HIP et la couche réseau :

La Séparation des deux niveaux transport et réseau l'un de l'autre nécessite un élément intermédiaire conservant cette relation, à cet effet l'architecture HIP spécifie un mécanisme de translation dynamique entre l'identificateur HI *"host Identifier"* et les différentes adresse(s) IP

qui constitue le nœud et vise versa (figure 5.2) de cette façon l'adresse IP reste un élément pure pour le routage des données

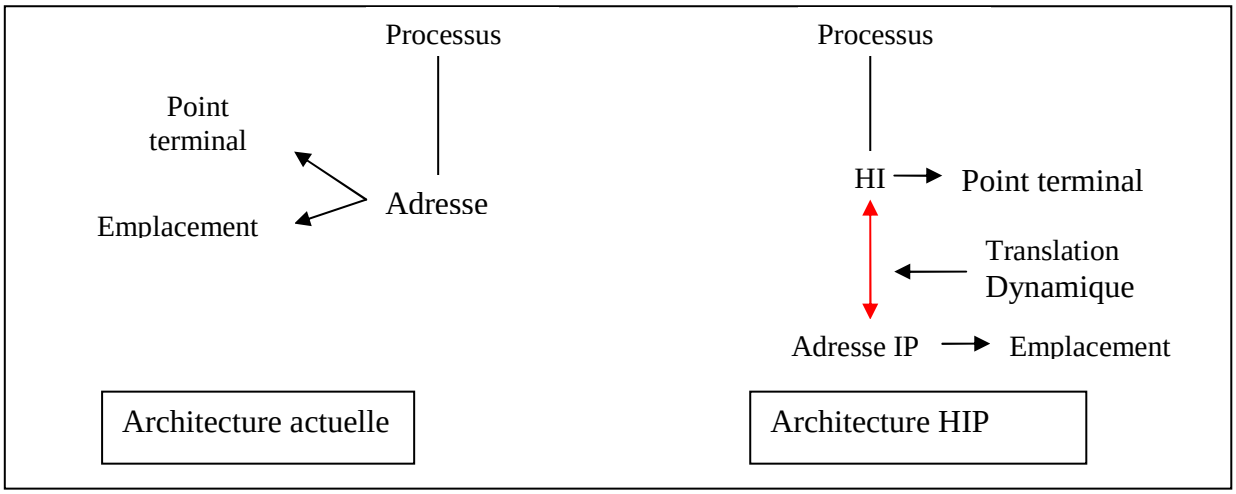


Figure 5.3 : HIP et la couche réseau

L'avantage de cette solution s'il y a un changement d'adresse au niveau d'un nœud (cas de mobilité) ou ajoute d'une autre adresse cela n'affecte pas la session ouverte entre les deux noeuds, cette changement affecte seulement la fonction de routage de l'information

5. Les identifiants d'hôtes :

Dans la spécification HIP, le HI est un élément cryptographique auto-généré par le nœud. Chaque hôte génère une clé celle-ci fonctionne comme un identifiant d'hôte HI "host Identifier" représenté par la clé publique d'une paire de clés, la clé secrète reste confidentiel et ne pas publier vers le réseau L'avantage de Cette HI est auto-certifié dans le sens peut vérifier les signatures sans l'accès d'une infrastructure clé-publique, ce qui rend cette solution adéquat avec les réseaux sans infrastructure ad hoc

Chaque hôte du réseau peut utiliser un algorithme distinct pour génère son HI, ceci peut résulte des HI avec des tailles différent, ce qui est inconvenable dans les échanges des données, pour surmonter ce problème dans notre étude, chaque nœud génère simplement un nombre entier qui joue le rôle d'un identifiant, cet identifiant est de longueur de 128 bit, avec cette propriété nous préservons la même structure d'une adresse IP

6. Initialisation d'une communication avec HIP :

Pour établir une session entre deux entités HIP spécifie quatre étapes sécurisé base sur un échange de clé Diffie-Hellman [RFC 2631] afin de crée une clé symétrique partagé par les deux parties, cette clé utilise pour crypter les données dans les paquets. L'implémentation de cette architecture sur un simulateur est plus compliquée, pour cela nous avons pris le principe de cette architecture, où chaque nœud est identifié par un identificateur unique qui est HI indépendant de l'adresse IP.

7. HIP et la gestion du Multi homing :

Parmi les défis derrière le développement de la couche HIP, le problème de multihoming dans les réseaux IP, car le basculement du transfert d'une interface vers l'autre

implique un changement d'adresse, ce qui peut perturber la session au niveau transport , dans la spécification du HIP, quand un nœud change ou ajouter une adresse IP (cas du mobile IP), cela traduit par le mécanisme correspond UPDATE [5], dans le cas où le protocole de transport utilisé est le SCTP les différentes adresses IP sont annoncées durant la phase d'établissement de l'association

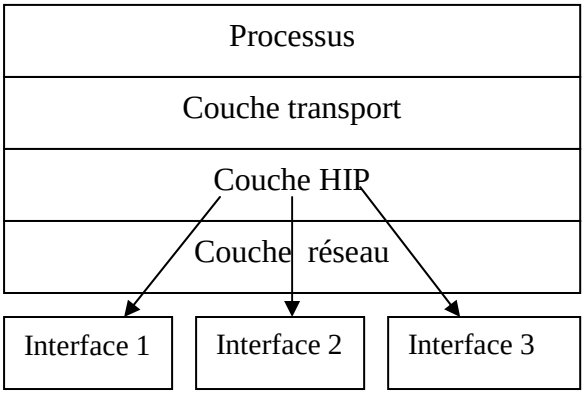


Figure 5.4 HIP avec un nœud multihomed .

Donc avec cette architecture une association SCTP multihomed, est identifie par le couple « HI source numéro de port », au lieu de « adresse 1, adresse2,…numéro de port » voir chapitre 4), de cette façon le changement d'une adresse n'affecte que le routage des données et l'association SCTP reste ouverte.

Simulation

Dans notre simulation nous avons définis un réseau ad hoc de quatre nœuds multihomed, chaque nœud est constitue de deux interfaces réseau, les chemins entre la source et le destinataire sont des chemins disjoints en noeud. Pour assurer cette propriété nous utilisons la technique de routage définit dans [11], et deux scénarios différents sont utilisé l'un utilise une topologie standards et l'autre une topologie modifié avec HIP figure 5.5. Le but de cette simulation est de voir le comportement de chaque scénario lorsqu'il y a une rupture dans la route.

Le grand travail dans cette simulation situe au niveau du simulateur NS2. Pour modifier l'architecture TCP/IP dans NS2, nous utilisons le patch NS-MIRACLE [12], cet outil nous permet d'introduire des modifications sur l'architecture du TCP/IP dans n'importe quel niveau dans le simulateur NS2

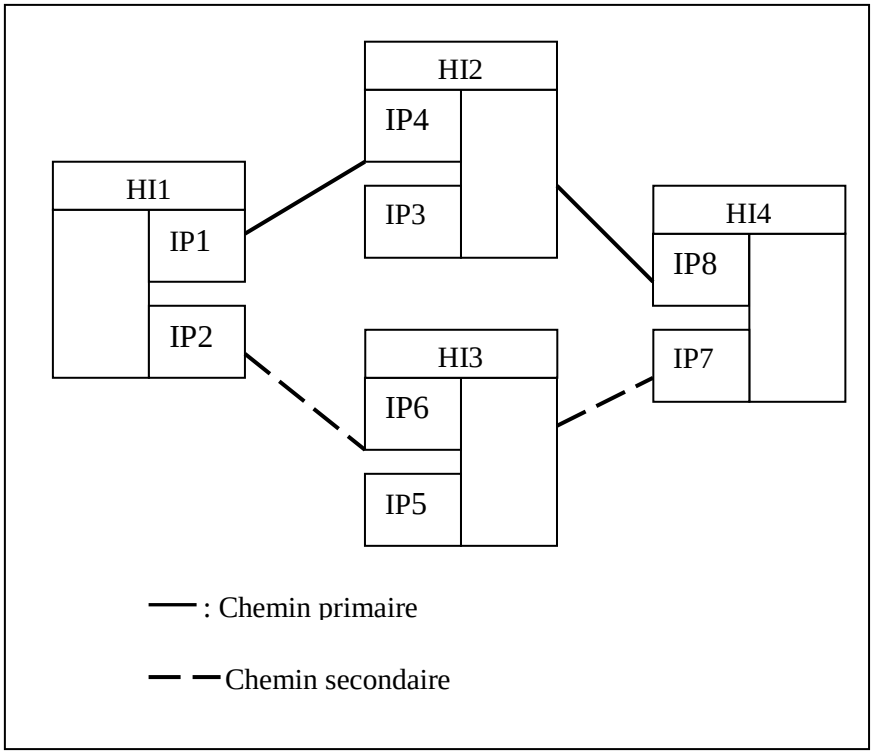


Figure 5.5 : scénario de la simulation

Les résultats de la simulation sont montrés dans la figure 5.6 :

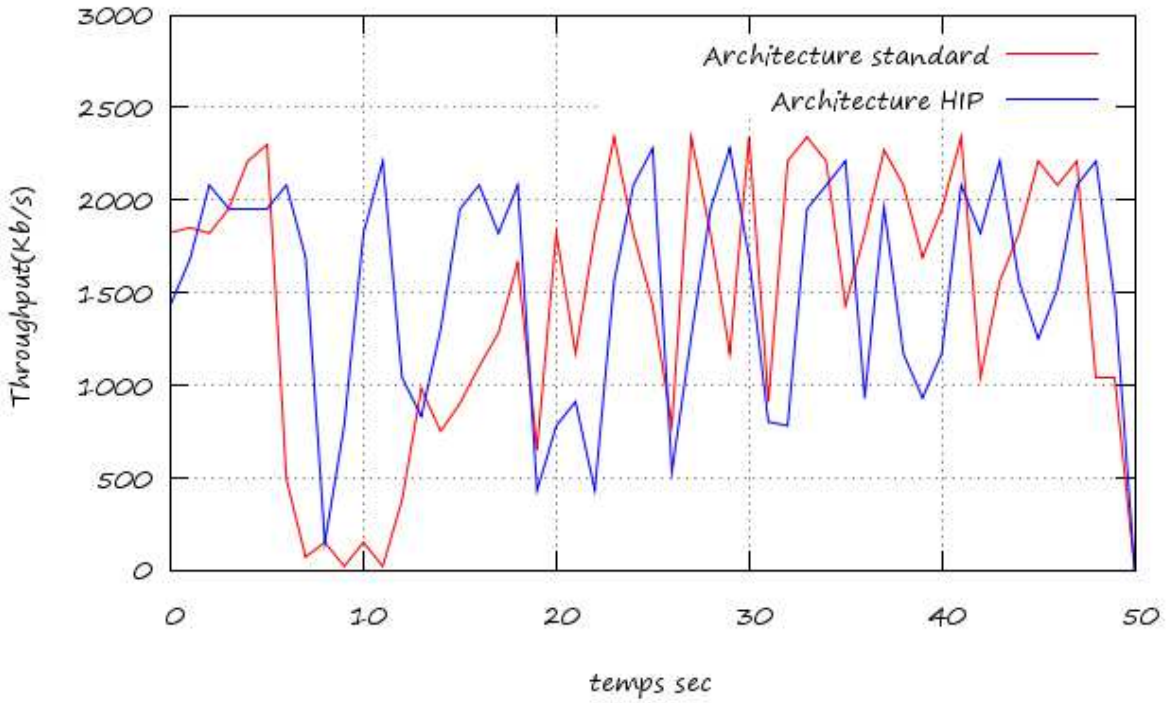


Figure 5.5 comparaison entre l'architecture HIP et standard quand il y a une rupture la route

D’après les résultats de la simulation nous remarquons :

- Pour le cas d’une architecture standard : lorsque le chemin il y a une perturbation de transfert lorsque le nœud 2 ce ceci est du d’une difficulté de commutation vers le chemin secondaire

- par contre dans le cas où l’architecture est optimisée avec HIP, nous remarquons qu’il y a seulement un baissement de transfert, ce qui prouve que l’opération de commutation entre le chemin primaire et alternatif déroulera d’une manière transparente et n’affecte pas la session ouverte

Conclusion :

La nouvelle architecture HIP est solution intéressé par la communauté Internet, car elle peut résoudre de nombreux problèmes existe dans l’architecture TCP/IP actuelle, tel la sécurité, la mobilité et le multihoming Appliquer cette couche tel qu’elle est dans les réseaux ad hoc nécessite un effort de plus pour l’adapter, car elle repose sur des notions complexes de la cryptographie et des entités centralisées tel le (DNS, PKI) qui sont dépourvu dans ces réseaux.

Dans ce travail nous avons appliqué le principe de cette architecture par la création d’un nouvel identificateur autre que l’adresse IP, et limiter le rôle de l’adresse IP seulement à l’opération du routage, dans la simulation cette solution prouve son efficacité aux différent défauts de la route, nous remarquons qu’il y a un baissement de transfert du de changement de chemin vers le destinataire, contre il y a une perturbation durant le passage de l’adresse

Référence :

[1] Moskowitz R., P Nikander. RFC 4423 "*Host Identity Protocol (HIP) Architecture"*, Mai 2006

[2] E.Borgia, M.Conti, and F.Delmastro "MobileMAN: Design, Integration, and Experimentation of Cross-Layer Mobile Multihop Ad Hoc Networks" IEEE Communications Magazine 2006

[3] L.GAVRILOVSKA "Cross-Layering Approaches in Wireless Ad Hoc Networks" springer 2006

[4] Moskowitz, et al RFC 5201 "Host Identity Protocol" avril 2008

[5] P. Nikander et al RFC 2506 "End-Host Mobility and Multihoming with the Host Identity Protocol" avril 2008

[6] M. Sarela, P.Nikander "Applying Host Identity Protocol to Tactical networks" journal IEEE 2008

[7] C.Perkins "Mobile IP" Journal IEEE may 2002

[8] T.Aura, A. Nagarajan and A. Gurtov "Analysis of the HIP Base Exchange Protocol" In Lecture Notes in Computer Science 2005, Volume 3574 pp. 481-494, 2005.

[9] R.J.W. Wilterdink "Host Identity Protocol: A state of the art research" 4th Twente Student Conference on IT, Enschede 30 January, 2006

[10] M Ratola, "Which Layer for Mobility? Comparing Mobile IPv6, HIP and SCTP", Helsinki Institute for Information Technology, 2004.

[11] Ki-Il Kim "A Cross Layered Approach for Multihoming on SCTP in Mobile Ad Hoc Networks" journal IEEE 2007.

[12] http://telecom.dei.unipd.it

Chapitre 6 :

Le Multi homing dans les réseaux satellitaires

1. Introduction :

Les réseaux satellitaire, actuellement fournis des services tel que la télévision, la radio, la téléphonie et les services de navigation. Un satellite offre une capacité de diffusion à large couverture, c'est-à-dire qu'il peut retransmettre les signaux captés depuis la terre vers plusieurs stations. La démarche inverse peut également être effectuée ; il peut récolter des informations venant de plusieurs stations différentes et les retransmettre vers une station particulière. L'architecture TCP/IP en couches été conçu pour être indépendante de toute technologie réseau afin qu'elle puisse être adaptés à toutes les technologies réseaux disponible [1], cependant les premiers satellites étaient passifs, ils ne font que refléter les signaux provienne des stations terriennes. Ses faiblesses est que les signaux ont été dispersés dans toutes les directions et peut être reçu par toute personne dans le monde, tard des satellites actifs mis en service, ces satellites ayant leur propre système émission/ réception. Telstar 1 fut le premier satellite actif qui a été mis en orbite [17], ces satellites peut être considéré dans l'architecture TCP/IP comme une sorte de relais hertzien, il ne s'occupe pas de la compréhension des données ou de routage, son rôle est de régénérer le signal qu'il a reçu et de le retransmettre amplifié en fréquence à la station réceptrice,

Récemment, une révolution dans l'industrie des engins spatiaux, le projet IRIS "**Internet Routing in Space"** [16],[20] est le fruit des recherches entre l'agence spatial NASA et Cisco system, ces deux compagnes développent des routeurs mobile embarqués sur satellite, en remplacent les routeurs sur les NCC "Network Contol Center" ce routeur avec son logiciel intégré on bord, et qui peut configurer depuis un NCC permet un assignement flexible de la bande passante à la demande des applications entre les utilisateurs dans des zones dispersés sans configuration statique [20] ainsi avec le développement des transmissions directe inter-satellite (ISLs) ceci permet de router le trafic IP sur le bord du satellite, l'avantage principale de cette technologie est d'éliminer le double-passage par le NCC et éviter la commutation par circuit. Ainsi le codage de l'information augmente la robustesse face erreurs Le routage du trafic IP nativement sur les satellites permet d'augmenter le débit, réduire le délai entre les points terminaux.

But :

Dans ce chapitre nous avons étudié les performances du protocole SCTP sur des liaisons satellites, notamment les propriétés de Multistreaming et de Multihoming qui peuvent améliorer la transmission par satellite et ainsi faciliter l'opération du handover inter-satellites. Notre étude s'articule sur les travaux de M Attiquzzaman [6],[11][15], professeur à l'université d'Oklahoma, et rédacteur en chef du journal "Network and Computer Applications". Beaucoup de ses activités de recherches sont soutenus par la NSF, la NASA et l'US Air force [19].

2. Les catégories des systèmes satellitaires :

Les satellites sont classés selon la hauteur de l'orbite où sont ils injectés, nous distinguons les GEOs **"**Geostationary Earth Orbit**"**, MEOs "Middle Earth Orbit**"** et les LEOs "Low Earth Orbit**"**, un satellite GEO apparaissent comme stationnaire, il tourne autour la terre avec même vitesse angulaire de la terre et dans la même direction ce qui facilite leur gestion,

cependant les satellites MEOs et LEOs sont apparu comme mobile par apport à un référence terrien.

3. Caractéristiques d'un lien satellite :

Les satellites de télécommunication transmettent donc des informations d'un point à l'autre de la Terre, dans un mode diffusion pour des programmes télévisés ou point à point pour des communications téléphoniques ou de données. Un satellite de télécommunication, il est constitué de différents *transpondeurs* qui reçoivent, amplifient et retransmettent des signaux sur des fréquences différentes [4]. Les satellites utilisent des bandes de fréquence particulières; les plus communes sont les bandes C, Ku ou plus récemment la bande Ka.

Le médium satellite a donc des caractéristiques particulières qui porte soit un avantage (large couverture) ou un inconvénient (faible SNR, haut BER) en résume ces caractéristiques :

- une grande couverture pouvant aller du tiers de la planète pour un satellite GEO, plus une accessibilité totale dans la zone de couverture, ce qui a permis de conserver cette technologie, non dépendante de facteurs terrestres (montagnes ou autres);
- large bande passante :
- long délai de propagation : le délai sur les liens satellites est influencé par plusieurs facteurs dont le principale est le type d'orbite [7], sans considérer le traitement du signal on-bord, en orbite basse le délai est de l'ordre 20-25 ms, cette valeur augmente à 110-150 ms pour un orbite moyen, et aller jusqu 'à 250-280 ms pour un orbite GEO.
- problèmes de couverture des zones polaire : ce problème pose pour les satellites GEOs les zones polaires situées au dessus de 81° de latitude n'étant pas couvertes.
- forte puissance requise **:** le couple mobile, satellite chaque un nécessite un émetteur à haute puissance.
- possibilité de réutiliser les fréquences : les satellites MEOs divisent la zone de couverture en petites cellules, cette découpage présente un avantage, la même fréquence attribuée dans une cellule peut être réutilise dans d'autres cellules
- forte atténuation du de l'effet atmosphérique et l'absorption du signal pour certaines plages de fréquences [4]
- un rapport BER plus élevé de l'ordre 10^{-6} pour un canal non codé [7]. Remedier ce problème il une amélioration consiste d'utilise des codeurs FEC ou convolutif un taux d'erreur de l'ordre de 10^{-9}.

4. Handover dans un environnement satellitaire :

Les systèmes satellites LEOs ont des avantages importants sur les systèmes GEOs en tant que composante de la prochaine génération Internet [15]. Il s'agit notamment de délai de propagation acceptable, assez de puissance requise pour la transmission sur le couple satellite/ terminal utilisateur, ainsi ces systèmes fournissent une allocation plus efficace du spectre en raison de la réutilisation fréquence entre les différent cellules ou faisceaux satellites. Cependant, en raison aux caractéristiques non géostationnaire et ses grande vitesse mouvement, la gestion de la mobilité dans les systemes LEOs est beaucoup plus difficile que dans les systèmes GEO ou MEO

D'augmenter la capacité de La gestion du Handover passe par trois étapes [14] : l'initialisation, la décision et l'exécution, pour l'initialisation soit le terminal ou le réseau peut effectue les mesures, mais l'un des deux peut décide.

- **Handover intra-satellite :** il correspond à un handover qui s'effectue entre deux cellules gérées par le même satellite.
- **Handover inter-satellite :** Cette situation est directement liée à la mobilité du satellite ou des stations dés que le handover s'exécute le client est pris en charge par une cellule dépendant d'un autre satellite

Le premier type de handover est assez simple, en ce sens qu'un seul et même satellite gère les deux cellules. Un handover inter-satellite est nettement plus complexe, car il faut gérer la communication entre les deux satellites sans interruption. Avec les satellites de type IRIS le traitement du handover non plus au niveau liaison mais aussi au niveau réseaux, et la gestion devient semblable à la gestion au par le protocole mobile IP

5. L'accès Internet /Intranet par satellite :

Le VSAT (Very Small Aperture Terminal) ou la norme DVB-RSC sont des exemples de l'accès à des services Internet via une liaison satellite depuis un PC équipé d'une antenne parabolique set opère dans la bande de fréquence C et Ku, chacune propose une architecture distincte:

5.1 Connexion par satellite unidirectionnelle :

Dans cette architecture la liaison satellite est utilisée d'une façon unidirectionnelle c'est-à-dire seulement dans la voie descendante cependant l'émission demande une connexion terrestre tel que DSL, le client doit s'abonner auprès un fournisseur d'accès Internet, celui si qui va redirige la requête vers l'Internet et renvoie les résultats par liaisons satellitaire vers le client, cette architecture implémenté dans le système DVB-RSC, l'avantage de cette architecture simple et ne demande assez de matériels spécifiques

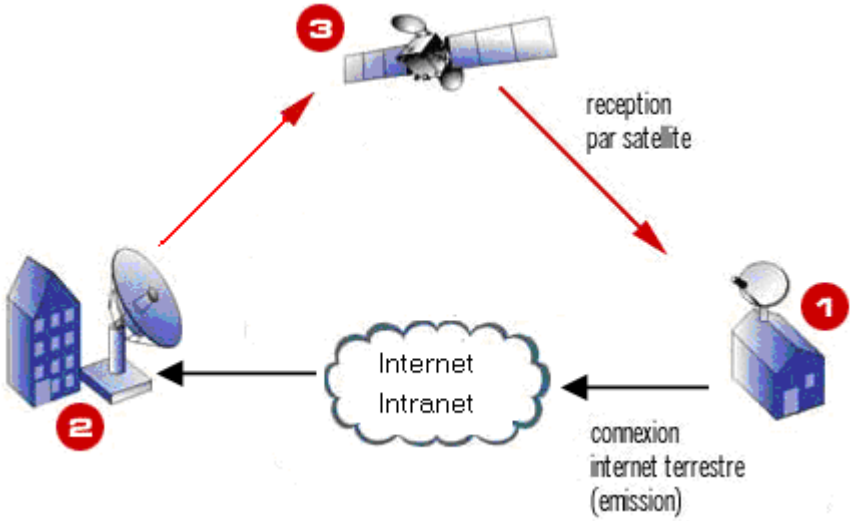


Figure 6.1 connexion TCP/IP par satellite unidirectionnelle

5.2 Connexion par satellite Bidirectionnelle :

Cette architecture est procurée par la technologie VSAT par les compagnes pétrolière des bases dispersées dans le monde Shell, Schlumberger, offre un débit allez jusqu' 20Mbit/s

pour la voie descendante, ici l'opérateur Internet par satellite bidirectionnel reçoit la requête de client par satellite, récupère le résultat de la requête sur l'Internet/Intranet, puis il le retransmet par satellite. L'avantage de cette solution ne demande aucune infrastructure chez le client, ou dans des zones qui non desservies par aucun des moyens de raccordement de données haut débit

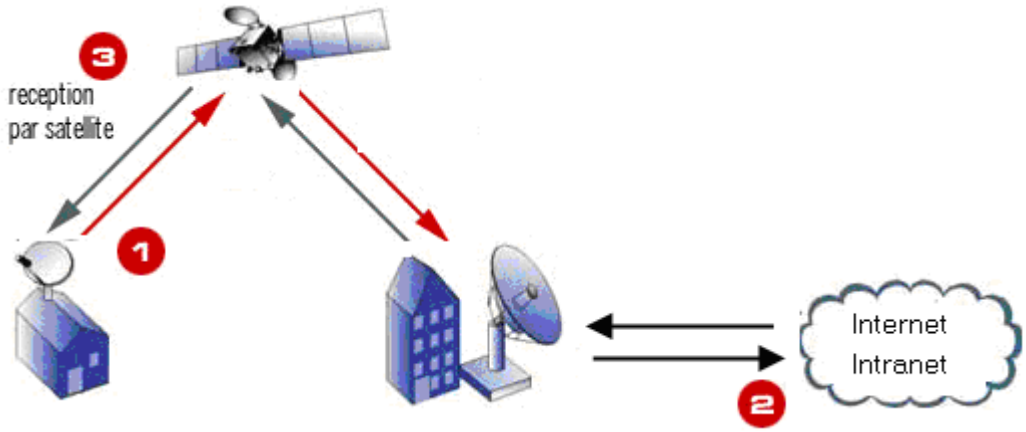


Figure 6.2 : Connexion TCP/IP par satellite Bidirectionnelle **:**

6. Les techniques d'accès au satellite :

Le multi-accés permet aux utilisateurs de partagent les ressources coûteuses du satellite bande passante, transpondeurs et puissance, sans aucune interférence entre les différents canaux. La différence essentielle avec les interfaces radio des réseaux de mobiles provient du long délai de propagation entre l'émetteur et le récepteur, les stations terrestres qui émettent des signaux ne peut informées que d'une éventuelle collision de leur paquet que 270 ms après l'émission.
Contrairement aux réseaux locaux, les réseaux satellite n'ont pas donné lieu à une normalisation spécifique. Plusieurs protocoles ont été proposés, mais aucun ne s'est vraiment imposé, cependant les techniques d'accès pour les réseaux satellite sont généralement classées en quatre catégories [2], [5]

6.1 Les méthodes de réservation fixe :

Les techniques d'accès FDMA : Frequency Division Multiple Access, TDMA : Time Division Multiple Access, ou CDMA : Code Division Multiple Access, sont techniques de réservation fixe réalisent des accès non dynamique et ne dépendent pas de l'activité des stations.

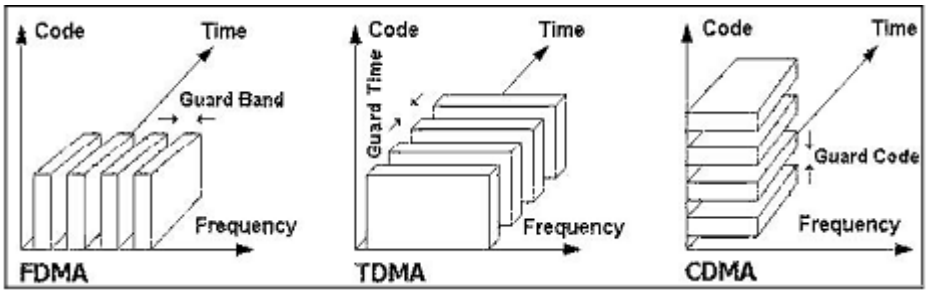


Figure 6.3 : les méthodes d'accès FDMA, TDMA et CDMA

SDMA Space Division Multiple Access : Cette méthode utilise des antennes directionnelles [9] cela permet aux stations d'émettre dans une direction sans interférer les signaux des autres stations

6.2 Les méthodes d'accès aléatoire :

Les techniques d'accès aléatoires donnent aux utilisateurs la possibilité de transmettre leurs données dans un ordre sans un assignement préalable du canal partagé. En revanche, ces techniques ne garantis aucune qualité de service, ainsi le nombre important des collisions gaspille et dégrade la capacité du canal, leur point fort réside dans une implémentation simple et un coût de mise en œuvre assez bas. Les deux grandes catégories de politiques d'accès aléatoires sont l'aloha et l'aloha discrétisé :

6.2.1 ALOHA :

Elle représente le schéma le plus simple de l'accès aléatoire, Quand un hôte détient un paquet à transmettre, il l'envoie, s'il ne reçoit pas d'acquittement au bout d'un temps, donc il considère qu'il y a eu collision, le hôte patiente un temps aléatoire T et retransmettre le paquet. Ce processus est répète jusqu'au succès de la transmission du paquet. Cette méthode ne nécessite pas d'une synchronisation mais les collisions sont inévitables

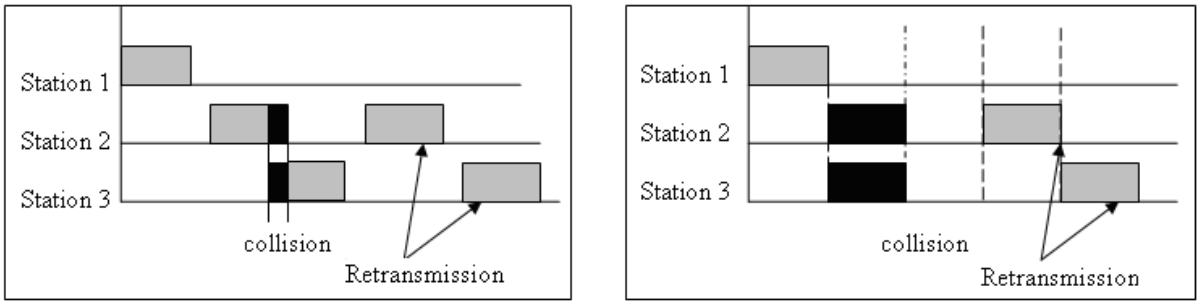


Figure 6.4 La gestion des collisions dans les méthodes d'accès *ALOHA, S-ALOHA*

6.2.2 Slowted-ALOHA :

C'est la version synchronisé d'ALOHA, elle conçu afin d'augmenter la capacité du système ALOHA pure en réduisant le nombre des collision partielles [8], dans cette technique le temps est découpé en tranches ou slots, où la durée d'un slot est supérieur à la durée d'un trame, alors, chaque machine veut transmettre doit attendre sa part dans la file de temps. Les collisions ici se produisent sur l'ensemble de la tranche et non plus sur des parties de paquets.

La figure ci-dessous trace les performances des mécanismes de ALOHA et S-ALOHA, il apparaît clairement que les meilleurs performances sont obtenus avec le protocole S-ALOHA avec :

Le débit de l'information donnée par l'équation suivante [8]

$S=G.e^{-2G}$; où :

S : le débit du canal
G : le trafic total écoule dans le réseau

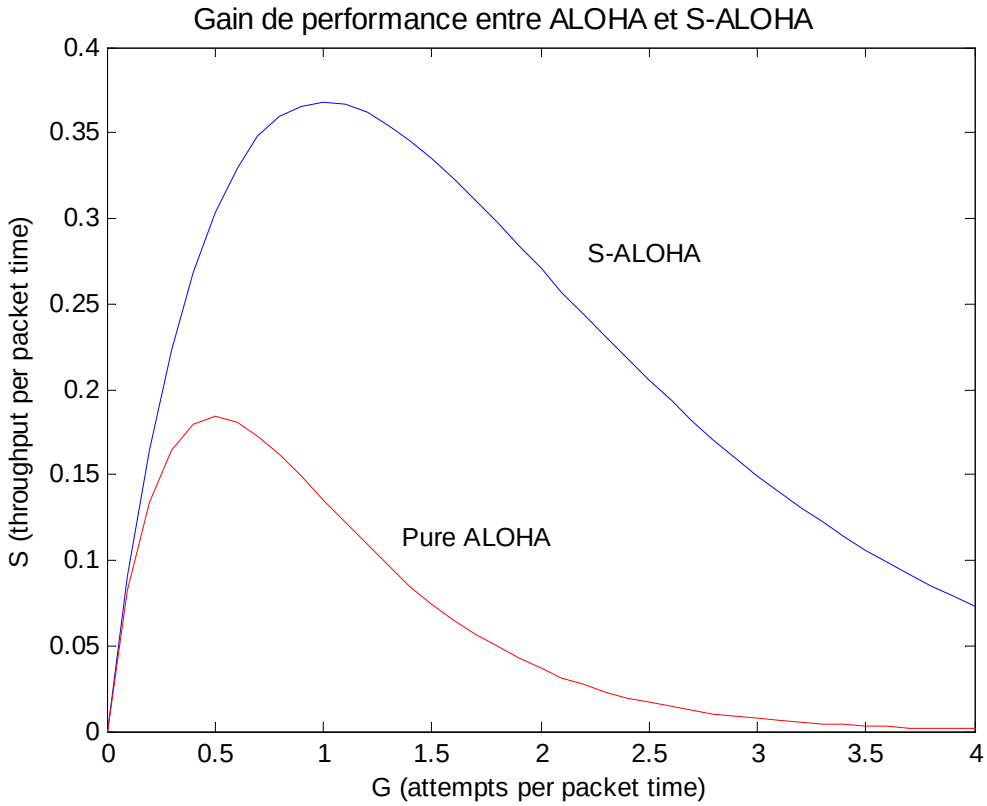


Figure 6.5 Le gain de performance entre ALOHA et S-ALOHA

6.3 Les méthodes de réservation par paquet PR:

L'avantage de ces méthodes evitent les collisions par l'utilisation d'un schéma de réservation de niveau paquets. De nombreux politiques existent, le dominateur commun de ces méthodes réside dans la faculté de réserver à l'avance des tranches de temps pour les stations qui ont des paquets à émettre. Une station ne peut émettre que si elle effectue une réservation, l'une de ces méthodes c'est R-ALOHA [18]

6.3.1 R-ALOHA :

Le principe de cette méthode c'est le découpage du temps en slots, une station *X* ne peut effectue une transmission qu'après une réservation d'un slot *M* dans la trame figure, si la réservation est réussie le slot *M* sera réservé à la station X durant sa transmission dans la trame, cependant les slots inoccupé sont libre à l'accès selon la méthode S-ALOHA

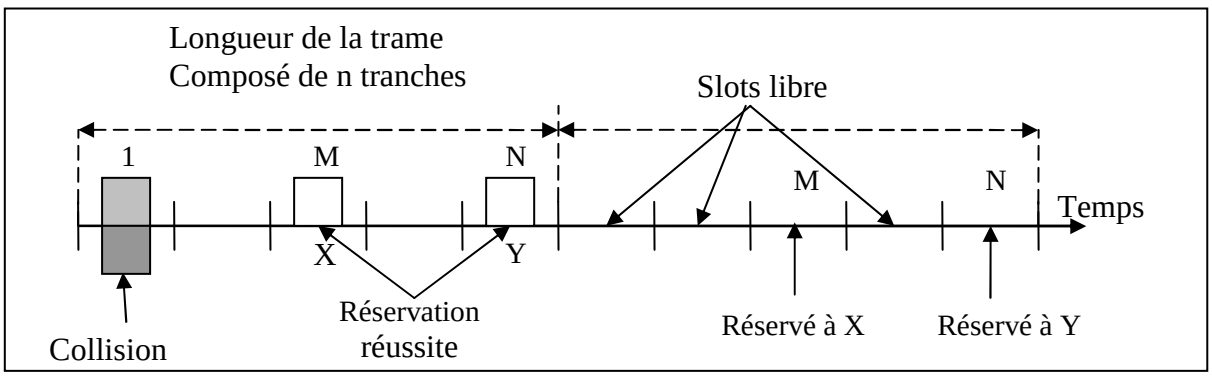


Figure 6.6 : La méthode d'accès ALOHA avec réservation

6.4 Les méthodes de réservation dynamique :

Les méthodes de réservation dynamique son objectif est de maximiser l'utilisation des ressources satellite, par assignement des ressources en fonction de la demande des utilisateurs. Des priorités peuvent attribuées aux différents utilisateurs. AD-FDMA et AD-TDMA [10] sont des exemples de réservation de ressources dynamique à la demande avec FDMA respectivement TDMA, On décrit ici la méthode DAMA.

6.4.1 DAMA

(Demand Assignment Multiple Access) : est un mécanisme d'allocation de ressources à la demande, spécifie dans le standard DVB-RCS [12], ce protocole fonctionne sous un mode centralisé (client /Serveur) permet aux STs de requérir régulièrement auprès de NCC ou d'un HUB (dans la terminologie VSAT) de la "capacité d'émission", c'est à dire des réservations de timeslots pendant lesquels ils pourront émettre sur la voie retour sans contention possible. Ces demandes de réservation de capacité sont calculées par le client DAMA installé au sein du ST selon l'état de ces files d'émission et transmises par des requêtes de capacité CR vers le serveur DAMA du NCC.

7. Le niveau transport pour les réseaux satellitaires :

Le transport des données sur des liaisons satellite issue d'un certains obstacles, ceci dépend du caractéristique du canal (long délai de propagation, faible SNR, haut BER..) et d'autres liés au comportement du TCP lui-même (slow-start, ACK..). Ceci impose l'IETF de produire un RFC (RFC 2488) spécifique pour le transport des données sur les réseaux satellites [21]. Un certain nombre d'améliorations ont été recommandé pour une utilisation TCP dans les réseaux satellitaire [7],[21]

Comme Le protocole SCTP dérivé de TCP ses caractéristiques et ses mécanismes tel que : les acquittements, contrôle de congestion, et contrôle de flot, SCTP hérite ces améliorations de TCP à l'addition de ces propres particuliers (multi-homing, multi-streaming), Cependant, comme décrit ci-dessous, la mise en œuvre de certaines de ces fonctionnalités dans SCTP sont différentes à celles du TCP.

7.1 Découverte MTU :

Le mécanisme MTU fournie à SCTP l'information sur la taille maximale lequel un segment SCTP ne subit à aucune fragmentation lors de son passage par différents réseaux, la différence avec TCP réside dans le nombre des chemins existent entre les deux entités. Une association SCTP dans le cas où les entités sont multi-homed peut avoir différents chemins,à cet effet SCTP choisis le plus petit MTU pour toutes les adresses IP du destinataire. Ce mécanisme de découverte est optionnel dans SCTP cependant son activation est recommandé pour les réseaux des satellites [6], car peut réduire l'overhead des paquets et augmente la taille de la fenêtre de congestion *cwnd* en terme de bytes

7.2 Les acquittements sélectifs SACK :

Les acquittements sélectifs pourvus une réaction robuste contre les pertes des blocs dans la même fenêtre des données, notamment dans les réseaux satellite qui se caractérise par un haut BER ce mécanisme permet d'éviter le retour vers l'état "Slow-start" et conserve la bande passante. L'utilisation des SACK (Sélective ACK) est obligatoire dans SCTP, ainsi le nombre de gap autorisé dans TCP trois ou quatre [6] reste insuffisant pour rendre compte tous

les segments perdus, donc les segments perdus ne peut pas être signalé dans un seul SACK,. à l'opposé le SCTP autorise autant de gap que TCP et le nombre est déterminé par le longueur du chunk et peut atteindre jusqu' au16.380 bloc

7.3 Fenêtre de réception plus large:

La taille de la longueur de la fenêtre dans l'entête TCP est 16 bit ce qui résulte une taille maximale de 65535 bytes cependant un canal DS1 GEO est de 96500 TCP ne peut exploite la totalité de la bande disponible d'une façon optimale, SCTP offre une longueur de la de 32 bit taille de la fenêtre peut atteindre

7.4 Taille initiale de la fenêtre de congestion :

Le document Internet RFC 2960 spécifie que la taille initial de la fenêtre de congestion $cwnd \leq 2$, si cette taille *cwnd* égale à 1 segment, Le récepteur doit attendre une duré de 200ms avant d'acquitter le premier segment et incrémente, ceci peut diminue le temps requis de démarrage slow-start par un cycle RTT

La table suivante résume les d SCTP et qui sont disponible dans TCP

Mécanisme	Utilisation	Emplacement
Découverte MTU	Recommandé	E
Slow-start	Obligatoire	E
Evitement de congestion	Obligatoire	E
Fast retransmit	Utilisation Implicite	E
Fast recovery	Utilisation Implicite	E
SACK	Utilisation Implicite	E, R
SACK	Recommandé	R
Large fenêtre récepteur		E, R

7.5 Effet de multistreaming :

Le but principal du multi-streaming, c'est d'éviter le problème du blocage HOL "Head-of-Line" au niveau des buffers du récepteur, due de la politique de gestion des arrivés dans TCP, ainsi le contrôle de congestion est appliqué à l'ensemble de streams et non à un stream indépendant, avec cette puissante propriété, le SCTP, créer :

- une indépendance entre les différents streams d'une association
- une indépendance entre la perte et la délivrance des paquets

La perte ou l'erreur des données dans un stream n'affecte pas les autres streams, ces derniers peuvent valider et passer à la couche application, les auteurs dans [11] ont évalué le SCTP - multistreaming sur des liens satellites, ils montrent que le multistreaming améliore les performances du SCTP en terme de Goodput, et ceci quand les buffers du récepteur de taille limitées. Ils ont aussi montré que le multi-streaming peut réduire les exigences des buffers au niveau du récepteur.

On note que le nombre de streams E/S est négocié pendant la phase d'initialisation et reste inchangeable durant l'existence de l'association SCTP, si on veut change le nombre de stream entre les end-points l'association doit être rétabli [13]. Le nombre de stream reste un sujet débat, sachant qu'un stream maintien un coût et une surcharge sur le réseau [13], donc le

nombre doit être choisi soigneusement avec le volume du trafic et les caractéristiques du canal.

7.6. Effet de Multihoming :

Le Multihoming comme décrit précédent, il refera à la situation où une machine ou un réseau est accessible à partir de plusieurs interfaces physiques, cette caractéristique qui est unique dans SCTP , TCP ne peut gère qu'une adresse IP (interface physique) un exemple de Multi-homing dans les réseaux satellitaire est montré dans la figure ci-dessous, où les deux points terminaux sont relier par deux liens satellitaires satellite1 et satellite 2

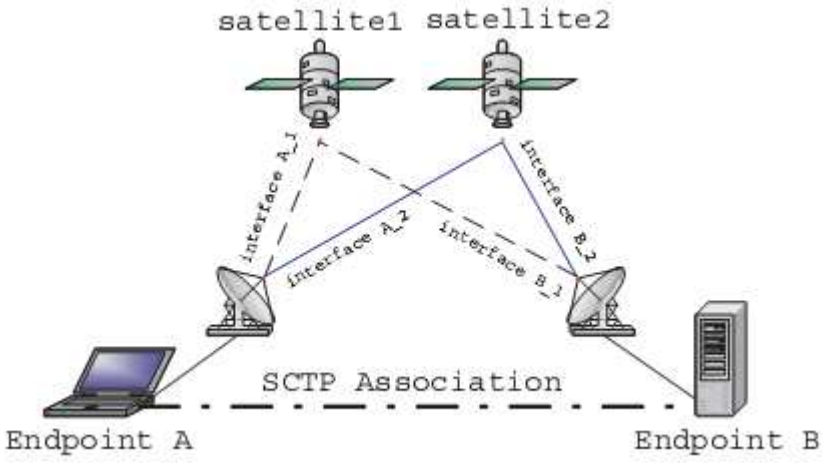


Figure 6.8 : le multihoming sur une liaison satellitaire

Une association SCTP entre des nœuds multi-homed, assure une commutation transparente vers un chemin alternatif, lorsque le chemin primaire devient inaccessible à cause d'un handover ou d'une période blackouts [6] L'autre avantage fournir par le Multihoming c'est quand il y a des erreurs ou de éventuelles pertes des paquets, l'émetteur peut effectue les retransmissions sur un chemin alternative, et évite de surcharge le chemin primaire.

Simulation :

Pour la simulation nous avons montré les performances du protocole SCTP sur une liaison satellite, la constellation définie est de type Iridium, les tables suivantes décritent les différents paramètres de la constellation Iridium et du protocole SCTP.

Paramètres	Iridium
Nombre des plans	6
Nombre de satellite par plan	11
Altitude	780 Km
Inclinaison à l'équateur	90°
Duré du période	100.4 min
ISLs par satellite	4
Lien montant	1.5 Mb/s
Lien descendant	1.5 Mb/s
BER du lien	10^{-4} à 10^{-9}

Table 6.1 : Caractéristique Constellation Iriduim

Type de trafic	FTP
Nombre d'association	De 10 à 40
Taille de entête	52 bytes
taille du paquet	512 bytes
Nombre de stream par association	1 à 4
Taille du buffer du récepteur	10 à 3000 bytes
Taille Initial de CWND	2 segments

Table 6.2 : différents paramètres du protocole SCTP

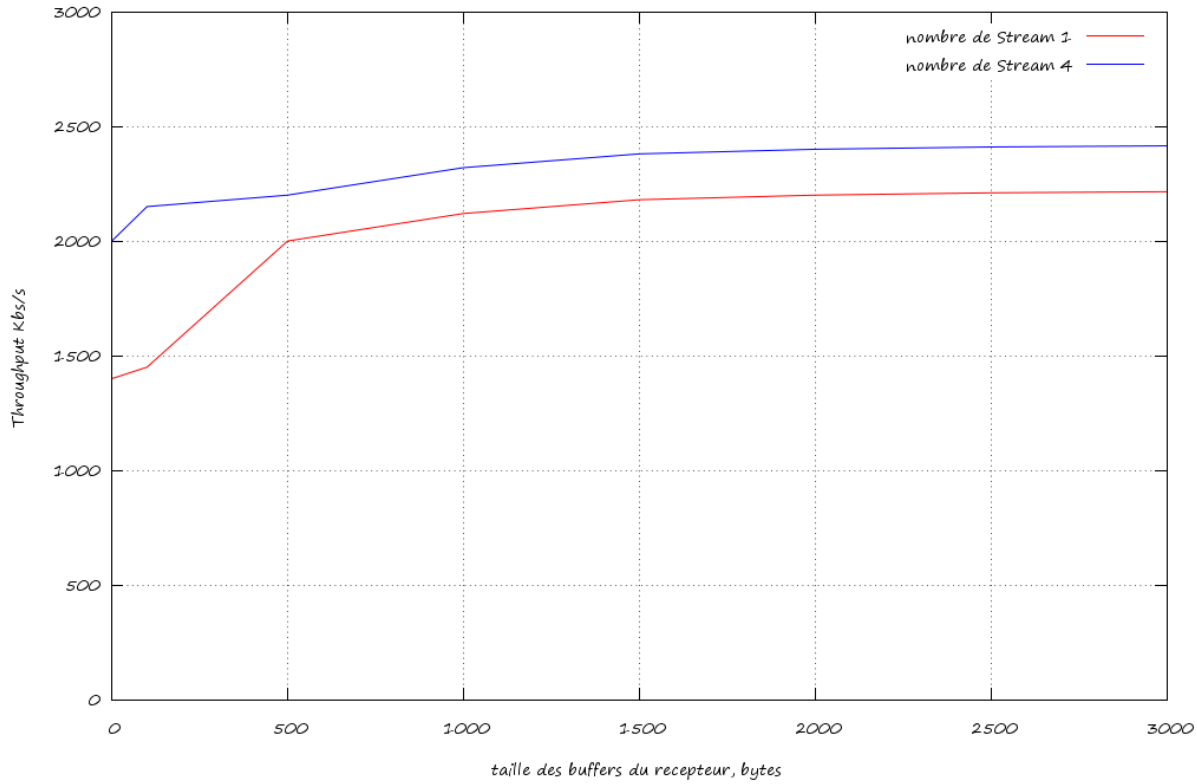


Figure 6.8 : Effet de nombre de streams sur une association SCTP

D'après les résultats nous remarquons que, le nombre de streams dans une association SCTP augmente le Throughut d'une communication, notamment si la taille des buffers est limitée, dans cette situation le problème du HOL "Head Of Line" peuvent être apparaître

La figure 6.9 montre Les performances d'une association multidomiciliés sur une liaison satellite, par rapport à une association standard, cette liaison est caractérisé par un haut BER compromis entre (10-9 et 10 -4) sachant qu'une association multidomiciliés, crée plusieurs chemins à la fois l'un est considéré comme un chemin primaire pour transférer des paquets de données et les autres sont des chemins alternatifs sont utiliser pour l'acheminement des paquets de contrôles ou pour la retransmission des éventuelles paquets perdus.

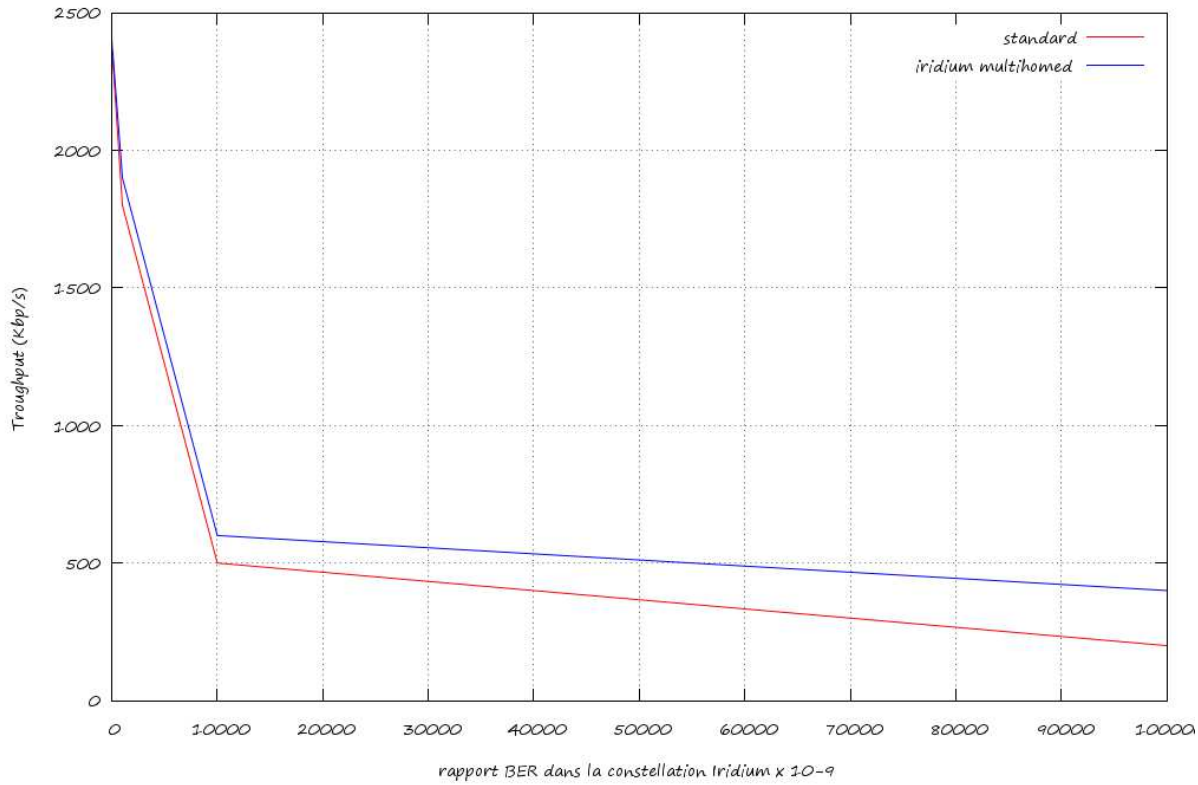


Figure 6.9 : effet du multihoming sur le débit d'une liaison satellite

10. Conclusion :

SCTP est un nouveau protocole de la couche transport défini par IETF, ce protocole détient des caractéristiques qui peuvent améliorer les communications dans un environnement spatial, nous commençons ce chapitre par une présentation des caractéristiques d'une liaison satellite (délai, taux d'erreur..) qui limite les performances d'un protocole de transport.

Les résultats de la simulation montrent que la propriété du multistraming améliore d'une manière significative les performances d'une communication satellitaire, notamment dans le cas où la taille des bufffers est limité ; l'autre cas quand nous utilisons des associations multidomiciliés, elles montrent aussi un comportement par rapport aux associations standards

Bibliographie :

[1] Z. Sun “Satellite Networking Principles and Protocols” edition Wiley 2005

[2] G. Pujolle " les réseaux " édition eyrolles 2008

[3] “The hand book of Ad-hoc wireless network “ CRC press édition 2002

[4] A.Scott “Understanding Microwave “ édition Wiley 1993

[5] G.E.Corazza “Digital satellite communication “ édtion Springer 2007

[6] S. Fu, M. Atiquzzaman and W. Ivancic “SCTP over Satellite Networks” journal IEEE 2003

[7] N. Ghani and S. Dixit “TCP/IP Enhancements for Satellite Networks” journal IEEE 1999

[8] A. Tanenbum “Computer Networks” fourth edition Prentice Hall 2003

[9] M.Cooper and M.Goldburg. “Intelligent Antennas: Spatial Division Multiple Access”. Annual Review of Communication page 999-1002, 1996

[10] G. Mara “VSAT Networks” edition Wiley 2003

[11] M. Atiquzzaman and W.Ivancic “Evaluation of SCTP Multistreaming over Satellite Links”

[12] F. Nivor, P Berthou, S. Abdellatif, TGayraud “Amélioration de l’Allocation Dynamique de Ressource dans un Système Satellite DVB-S/RCS” LAAS-CNRS, 2006

[13] S.Kang and M.Fields “Experimental Study of the SCTP compared to TCP” Technical Report, Department of Electrical Engineering,TexasA&MUniversity,2003

[14] R .Sheriff et Y.Hu “Mobile Satellite Communication Networks” edition John Wiley 2001

[15] M Atiquzzaman, S. Fu and W Ivancic “A Transport Layer Seamless Handoff Scheme for Space Networks”

[16] K.Leung,D.Shell,W.Ivancic,D.Stewart,T.Bell, and B. Kachmar “Application of Mobile-IP to Space and Aeronautical Networks” IEEE Aerospace and Electronic Systems Magazine, Dec2001.

[17] F. Houeto, C. Anato, R. Sagbo and J. Hounsou “VSAT Solution for Education”

[18] Simon .S lam “an analysis of the reservation – ALOHA protocol for satellite packet switching” journal IEEE 1978

[18] http://en.scientificcommons.org/mohammed_atiquzzaman , une collection d’articles de M.Atiquzzaman sur les solutions IP satellite

[19] http://www.ou.edu/coe/cs/Faculty/atiq.html page perso de M. attiquzzaman

[20] http://www.cisco.com/go/iris “Cisco Internet Routing in Space (IRIS) ”

[21] M. Allman, D. Glover and L. Sanchez “Enhancing TCP over Satellite Channels using Standard Mechanisms” RFC 2488, IETF 1999