République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Saad Dahlab Blida 1

Faculté des sciences

Département d'informatique

Mémoire Présenté par :

MANSOUR RIAD

En vue d'obtenir le diplôme de master

Domaine : Mathématique et informatique

Filière : Informatique

Spécialité : Informatique

Option : Ingénierie de logiciels

Sujet : Amélioration de la performance de TCP dans les réseaux mobiles ad hoc

Devant le jury :

ould Khaoua	President
Chikhi. I	Examinatrice
Mme. GHERIBI Hayet	Promotrice
Mr. DOUGA Yassine	Encadrant

Promotion : 2016/2017

Dédicaces

Je dédie ce modeste travail

À mes très chers parents que Dieu les garde

En témoignage de ma profonde gratitude et mon incontestable reconnaissance, pour leurs sacrifices, leur confiance qu'ils m'accordent et tout l'amour dont ils m'entourent.

À ma petite sœur « Romaissa ».

À mes frères « Mohamed » et « Farid » et « Abdelkader ».

À toute ma famille.

Et à tous ceux qui me sont chers.

Que Dieu vous garde.

M.Riad

Remerciements

Grâce à Dieu, nous avons abouti à la concrétisation de ce travail.

En préambule à ce mémoire, nous souhaiterons adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire.

Je remercie infiniment Mr. DOUGA Yassine notre encadrant pour son aide, sa patience et son attention durant cette année, on le remercie de nous avoir fait confiance et pour les informations très utiles qu'il a mis à notre disposition et on lui souhaite tout le bonheur et la prospérité.

On remercie également notre promotrice Mme. GHERIBI Hayet pour avoir accepté de nous encadrer tout au long de ce travail, pour son amabilité, sa disponibilité, son aide, ses conseils , ses suggestions et le temps qu'elle a bien voulu nous consacré malgré ses charges académiques et professionnelles.

On remercie tout nos enseignants qui ont contribué de près ou de loin à notre formation universitaire.

Enfin, nous ne saurons oublier dans ces remerciements tous ceux qui nous ont aidés pour mener à bien ce travail dans de bonnes conditions.

ملخص:

الطبيعة المتنقلة لعقد الشبكات المخصصة والوصلات الراديوية لا يمكن الاعتماد عليها دائما, يمكن أن تؤثر على حسن استقبال البيانات. قدمت بروتوكولات النقل مثل TCP لضمان انتقال البيانات بصفة موثوقة التي يمكن الاعتماد عليها في الشبكات السلكية أو فقدان حزمة يرجع أساسا إلى احتقان في الشبكات، قد تسيء تفسير هذه الأحداث وتسبب رد فعل TCP سيئة.

لمعالجة هذه الظاهرة واتصالات موثوقة، يحاول بروتوكول النقل TCP لتقديم أفضل الحلول، لكنه يعامل جميع الخسائر بنفس الطريقة من خلال التذرع آلية التحكم في الازدحام. ومع ارتفاع معدل الخسارة، يتحلل أداء برنامج التعاون الفني في الشبكات المخصصة.

وتقترح مجموعة من التقنيات لتحسين أداء بروتوكول TCPبشأن الاتصالات اللاسلكية من طرف إلى طرف. النهج المقترح هو دمج TCP آلية فقدان التمايز تستخدم قوة إشارة الاتصالات الجارية على أساس صلاحيات إشارات الاتصالات السابقة (استرداد إشارة من الطبقة المادية)، وهذا يهدف إلى التفريق بين الخسارة الناجمة عن الازدحام وذلك بسبب التنقل.

وأثبتت نتائج المحاكاة أن النهج المقترح يعطي أداء أفضل من نهج أوبونتو تكب (TCP رينو) في بيئة لاسلكية متنقلة.

الكلمات الرئيسية:

بروتوكول النقل، الازدحام، قوة الإشارة، النقل، محاكاة، TCPاوبينتو، الوسائط المتعددة، الصحة العازلة، عتبة.

Résumé :

La nature mobile des nœuds des réseaux ad hoc et les liens radios qui ne sont pas toujours fiables peuvent avoir un impact sur la bonne réception des données. Les protocoles de transport tels que TCP prévus pour assurer une transmission fiable dans les réseaux filaires ou la perte des paquets est principalement due à des congestions dans les réseaux, peuvent mal interpréter ces événements et engendrent une mauvaise réaction de TCP.

Pour remédier à ce phénomène et fiabiliser les communications, le protocole de transport TCP tente d'apporter les meilleures solutions, mais ce dernier traite toutes les pertes de la même manière en invoquant un mécanisme de contrôle de congestion. Avec un taux élevé des pertes, les performances du protocole TCP dans les réseaux ad hoc se dégradent.

Un ensemble de techniques sont proposées pour améliorer les performances du protocole TCP sur les communications sans fil de bout en bout. L'approche proposée est un mécanisme de différentiation de perte intégrer à TCP qui utilise la puissance du signal des communications en cours en se basent sur les puissances des signaux des communications précédentes (récupérer la puissance du signal à partir de la couche physique), ceci a pour but de faire la différence entre une perte due à la congestion et celle due à la mobilité.

Les résultats d'émulation ont prouvé que l'approche proposée donne de meilleures performances que l'approche TCP de Ubuntu (TCP Reno) dans un environnement sans fil mobile.

Mots clés :

TCP, Congestion, Puissance de signal, Transport, émulation, TCP de Ubuntu, Multimédia, buffer health, seuil.

Abstract:

The mobile nature of the nodes of the ad hoc networks and the radio links which are not always reliable can have an impact on the good reception of the data. Transport protocols such as TCP for reliable transmission in wireline networks or packet loss are mainly due to congestion in networks, may misinterpret these events and cause a poor TCP response. To remedy this phenomenon and make communications more reliable, the TCP transport protocol attempts to provide the best solutions, but TCP treats all losses in the same way by invoking a congestion control mechanism. With a high rate of loss, TCP performance in ad hoc networks degrades .

A set of techniques are proposed to improve the performance of the TCP protocol on end-to-end wireless communications. The proposed approach is a TCP loss differentiation mechanism that uses the signal strength of current communications based on the signal strengths of previous communications (recovering the signal strength from the physical layer). to distinguish between a loss due to congestion and that due to mobility. The emulation results proved that the proposed approach gives better performance than the Ubuntu TCP approach (TCP Reno) in a mobile wireless environment.

Keywords:

TCP, Congestion, Signal strength, Transport, emulation, Ubuntu TCP, Multimedia, buffer health, threshold.

Tables des matières

Listes des figures :

Listes des tables :

Abréviation :

Wpan : Wireless Personal Area Network

Wlan : Wireless Local Area Network

Wman : Wireless Metropolitan Area Network

Wwan : Wireless Wide Area Network

BLR : Boucle locale radio

WIMAX : Worldwide Interoperability for Microwave Access

GSM : Global System for Mobile Communication

GPRS : General Packet Radio Service

WIFI : Wireless Fidelity

MAC : Media Access Control

AP : Access point

IP : Internet protocol

TCP : Transport control protocol

UDP: User Datagram Protocol

DCCP : Datagram Congestion Control Protocol

SCTP : Stream Control Transmission Protocol

RTO : Retransmit Time Out

RTT : Round trip time

Syn : Paquet de synchronisation

ACK : accusé de réception

CWND : congestion window

HTTP : Hypertext Transfer Protocol

AIMD : Additive Increase and Multiplicative Decrease

DUPACK : ACK dupliqué

SACK : Selective Acknowledgment

OSI : Open SystemsInterconnection

RSSI : Puissance du signal reçu

ICMP : Internet Control Message Protocol

RRN : Notification de la restauration de la route

RFN : Notification d'erreur de route

BER : Erreurs de bits

ECN : Explicit Congestion Notification

COPAS: COntention-based PAth Selection

OOO: Livraison Out-Of-Order

TPSN : TCP Packet-Sequence-Number

ADSN : ACK de duplication de numéro de séquence

MIMD : l'augmentation multiplicative et la diminution multiplicative

PSMI : La puissance du signal minimale de la route

PSE: La puissance du signal estimé

MCPS : La moyenne de changement de la puissance du signal

Introduction générale :

L'évolution récente des technologies de communication sans fil et l'émergence de terminaux mobiles (portables, Smartphones, etc.) ont rendu possible l'accès au réseau partout et à tout moment, sans avoir besoin de brancher les appareils communicants à une infrastructure. Les réseaux ad hoc sont des réseaux sans fil dont les nœuds adjacents communiquent directement entre eux (sans intermédiaire).
Malheureusement ce type de communication sans fil peut être affecté à cause de plusieurs problèmes comme la dégradation de la qualité de signal ou le bruit, mobilité..., d'où les protocoles de la couche transport (modelé OSI) peuvent assurer la fiabilité de la communication.

TCP est actuellement le protocole de la couche transport le plus largement utilisé pour réaliser les transmissions de bout à bout fiables et ordonnées à travers l'internet [32]. Cependant, bien qu'il soit bien optimisé pour les réseaux filaires pour lesquels la perte de paquets est toujours considérée être provoquée par une congestion, TCP présente des limites quand il est appliqué aux réseaux sans fils. En effet, l'hypothèse implicite de TCP que toute perte de paquets est due à une congestion n'est plus valide dans les réseaux sans fil en particulier les réseaux mobiles ad hoc,où les erreurs du canal sans fil (interférence, perte du signal, la mobilité et le routage multi-chemin…) peuvent considérablement corrompreou troubler la livraison de paquets. Ce qui implique une iniquité et une dégradation des performances de TCP.

Plusieurs tentatives ont été faites pour améliorer la performance de TCP dans lesréseaux sans fil, mais aucune de ces approches n'a été normalisée. De plus, des recherches sont effectuées qui s'intéressent à la performance de TCP dans les réseaux mobiles ad hoc multi-sauts mais qui sont encore actives dans ce domaine et de nombreux problèmes sont encore ouverts.

L'un des plus grand inconvenants de la solution TCP Hybrid et ce malgré les bons résultats obtenu est l'apport du concept inter-couches ou cross-layer dans la solution proposée qui la rend difficile à implémenter dans une émulation. Quelque chose qui n'ont pas réalisable dans l'émulation car le modèle OSI marche dans une seul sens. L'objective principale de ce travail est de modifier l'approche [54], afin de l'implémenter dans le cas réel d'émulation en essayant de prédire les valeurs de puissance de signal de la communication en cours à partir des communications précédents sans descendre à la couche physique pour déterminer le vraie cause de la perte de paquets sur le réseau(congestion ,mobilité….) afin d'améliorer les performances de TCP dans les réseaux sans fil.

Ce document est organisé en quatre chapitres.

Chapitre 1 : notion de base, nous avons présentés des principes dans le réseau informatique, ainsi des définitions et des transactions liées aux comportements du protocole TCP.

Le chapitre 2 : état de l'art, nous avons présentés les différentes versions d'amélioration du protocole TCP dans les réseaux sans fil.

Le chapitre 3 : conception, le but de ce chapitre est de proposer une solution qui vise à implémenter la solution [54] dans un cas d'émulation.

Le chapitre 4 comporte deux parties, l'implémentation et l'évaluation de notre approche. La partie d'implémentation présente l'environnement de l'émulation linux (Ubuntu) et les différents schémas de notre émulation.

La partie évaluation est une présentation et une interprétation des résultats obtenus suite àl'émulation.

Chapitre 1

Notion de base

Chapitre 1 Notion de base

1. Introduction :

Le domaine sans fil a connu une croissance exponentielle durant cette dernière décennie. On constate un grand progrès dans les infrastructures réseau, la disponibilité des applications sans fil et l'émergence des appareils sans fil tel que les ordinateurs portables ou les ordinateurs de poches, et les téléphones cellulaires. Ces appareils jouent un rôle important dans notre vie. Ils ne sont pas seulement plus petits, moins chers, plus pratiques et plus puissants. Parfois et dans pas mal de situations, l'utilisateur sollicite une infrastructure qui n'est pas disponible ou elle ne peut pas être installée. Pour fournir une connectivité ou des services réseau dans ces situations, il est nécessaire d'utiliser un réseau ad hoc.

Dans le reste de ce chapitre, on présentera les éléments fondamentaux des réseaux sans fil, puis on décrira les réseaux ad hoc tout en présentant leurs défis et problèmes, après en commençant par une généralité sur le protocole de transport TCP, fonctionnement général du protocole TCP et à la fin les différentes versions de TCP.

2. Le réseau informatique :

2.1. Définition :

Un réseau est l'ensemble d'acteurs, d'agents économiques, de nœuds, ou de lieux de communication grâce auxquels les messages circulent. Selon *Guy Pujolle*, un réseau informatique: « désigne tout ensemble d'éléments capables de véhiculer de l'information d'une source vers une destination. Le téléphone en est la meilleure illustration » **[1].**

On appelle nœud (node) l'extrémité d'une connexion, qui peut être une interconnexion de plusieurs connexion (un ordinateur, un routeur, un concentrateur, un commutateur, un téléphone mobile,…..).

Les supports de communication entre les équipements peuvent être des câbles dans lesquels circulent des signaux électriques, l'atmosphère (ou le vide spatial) où circulent des ondes radio, ou des fibres optiques qui propagent des ondes lumineuses.

Les équipements sont connectés directement ou non entre eux, selon un type d'organisation connu appelé topologie réseau.

Les informations échangées sont standardisées grâce à l'utilisation des protocoles de communication unifiés entre les équipements du réseau. Ces protocoles sont des procédures qui contrôlent le flux d'information entre des équipements.

2.2. Les composants physiques des réseaux locaux :

2.2.1. Les équipement de réseau :

a- La carte réseau (carte LAN – Carte Ethernet) :

Elle est installée sur chaque équipement du réseau. Elle permet de faire communiquer les équipements entre eux .Elle prend en charge la détection des collisions sur un réseau Ethernet Les cartes réseaux ont une adresse physique unique attribuée par le constructeur.

Cette adresse, appelée adresse MAC (Media Access Control) est essentielle car elle permet à une machine d'être reconnue par les autres machines du réseau.

La carte réseau se présente sous la forme d'une carte d'extension connectée à un bus, elle comportant un connecteur RJ45, BNC, fibre ou un émetteur/récepteur sans fil [2].

b. Le concentrateur (Hub) : Servent à relier entre elles toutes les parties d'un même réseau physique, généralement tous les ordinateurs sont reliés à un Hub, sauf dans le cas d'un câblage coaxial où le Hub est inutile.

Lorsqu'une information arrive sur un Hub, elle est rediffusée vers toutes les destinations possibles à partir de celui-ci, c'est à dire vers toutes ses prises [2].

c. Le commutateur (Switche) :

Le commutateur (ou Switch) est un système assurant l'interconnexion de stations ou de segments d'un LAN en leur attribuant l'intégralité de la bande passante, à l'inverse du concentrateur qui la partage.

Les commutateurs ont donc été introduits pour augmenter la bande passante globale d'un réseau d'entreprise et sont une évolution des concentrateurs Ethernet (ou HUB) [2].

d. Le pont (Bridge) :

Un pont est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Ainsi, contrairement au répéteur, qui travaille au niveau physique, le pont travaille également au niveau logique (au niveau de la couche 2 du modèle OSI), c'est-à-dire qu'il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont [2].

e. Le routeur (Router) :

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règles. Il y a habituellement confusion entre routeur et relais, car dans les réseaux Ethernet les routeurs opèrent au niveau de la couche 3 du modèle OSI [2].

f. Le répéteur (Repeater) :

Un répéteur est un dispositif électronique combinant un récepteur et un émetteur, qui compense les pertes de transmission d'un média (ligne, fibre, radio) en amplifiant et traitant éventuellement le signal, sans modifier son contenu. Dans le domaine des télécommunications, un répéteur (de l'anglais transponder) désigne un canal de modulation exploité dans les transmissions radio, de télévision et de données numériques qui véhicule des signaux exploités dans d'autres fréquences d'émission [2].

g. Le passerelle (Gateway)

Sont des dispositifs permettant d'interconnecter des architectures de réseaux différentes. Elles offrent donc la conversion de tous les protocoles, au travers des 7 couches du modèle OSI.

L'objectif étant de disposer d'une architecture de réseau évolutive, la tendance actuelle est d'interconnecter les réseaux par des routeurs, d'autant plus que le prix de ceux-ci est en baisse [2].

3. Modèle OSI :

3.1. Définition :

Le modèle OSI, ou Open System Interconnection protocols**[3]** est un standard de communication, en réseau, de tous les systèmes informatiques. Les spécifications du modèle OSI ont été conçues et implémentées en 1984 par deux organisations internationales : l'International Organisation for Standardization (ISO) **[4]** et l'Internation Télécommunication Union (ITU). Le modèle de référence OSI décrit comment les informations issues d'un logiciel sur un ordinateur rejoint par l'intermédiaire d'un réseau, une autre application située sur un autre ordinateur. Le modèle OSI est un modèle conceptuel subdivisé en sept couches, chacune spécifiant une fonction du réseau particulière. Il permet de diviser les fonctions impliquées pour l'acheminement de l'information en sept groupes de tâches plus indépendamment gérables. Un groupe de tâches est donc associé à chacune des sept couches (physique, liaison, réseau, transport, session, présentation, application). Les tâches d'un groupe sont suffisamment bien définies de sorte qu'elles peuvent être implémentées de manière autonome. Ces couches sont présentées sur la figure suivante [Figure 1] On peut encore effectuer une subdivision entre les différentes couches en les classifiant entre les couches hautes et les couches basses. Les couches hautes traitent des caractéristiques

d'implémentation des applications et sont proches de l'utilisateur final, alors que les couches basses traitent du transport des données proprement dit.

Les couches 1, 2,3 et 4 sont dites basses et les couches 5,6 et 7 sont dites hautes sur la figure 1[5].

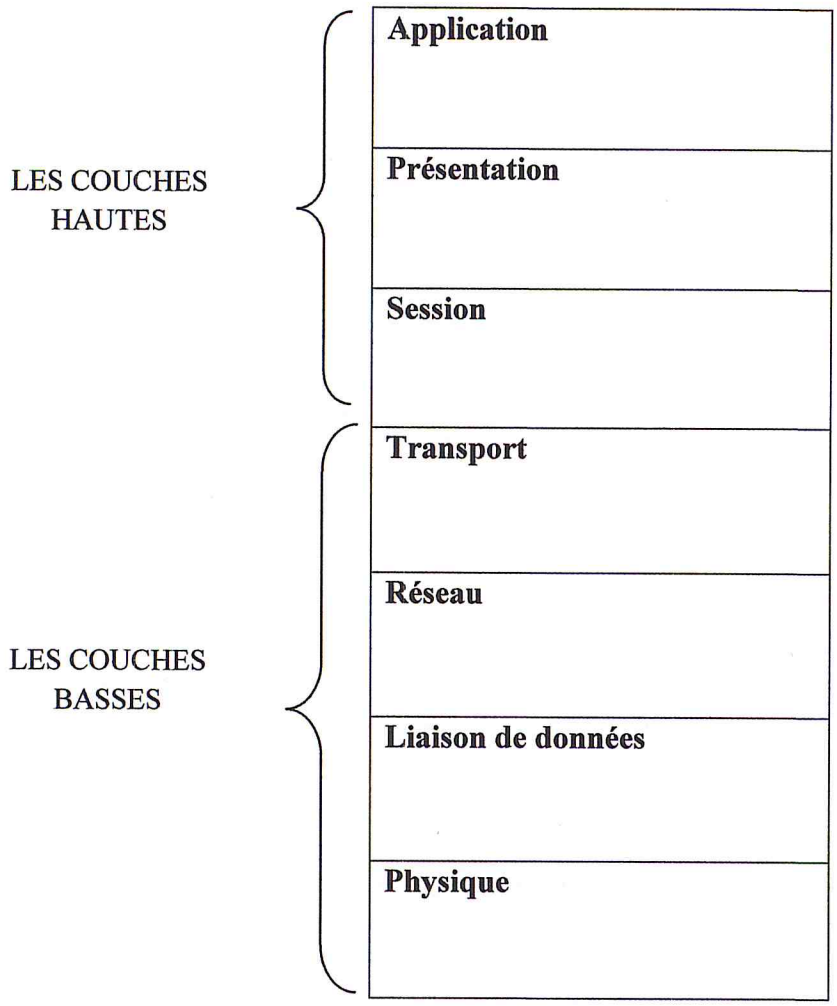

Figure 1: Le modèle OSI

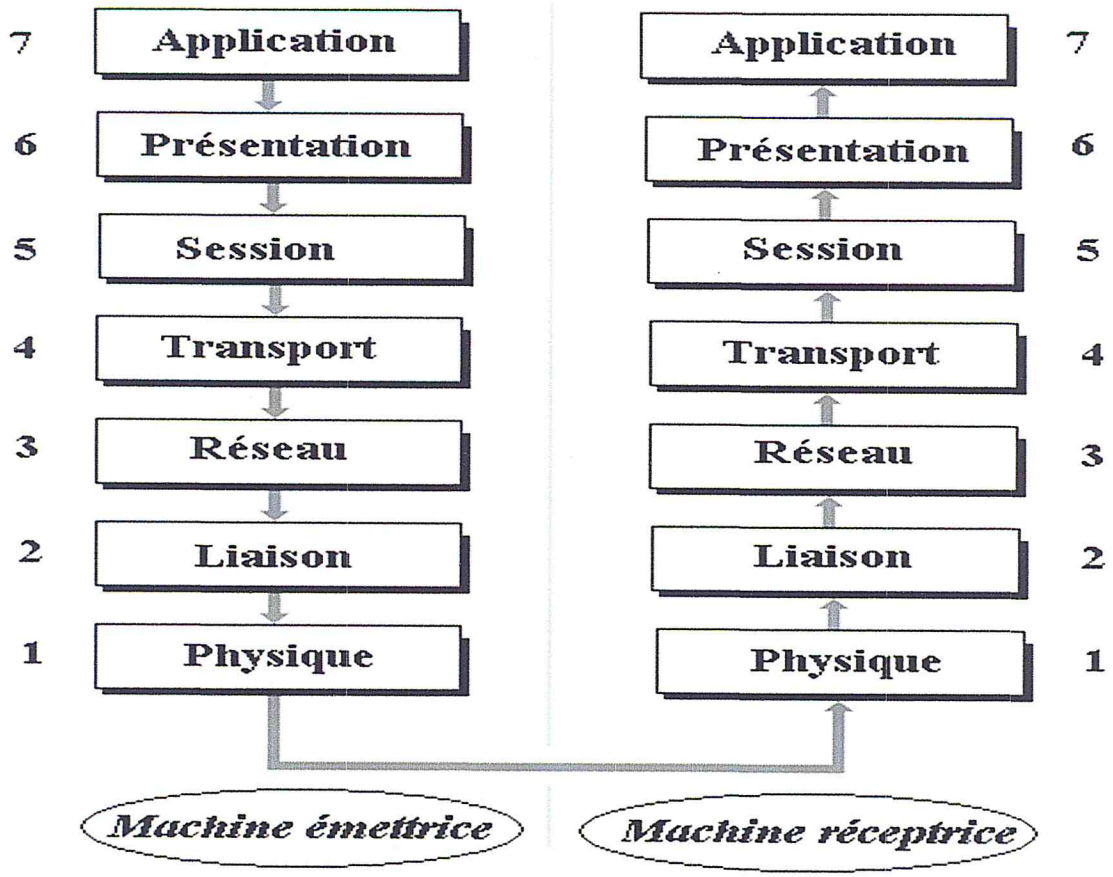

Figure 2: Le modèle OSI.

3.2. Les couche du modèle OSI :

Le modèle OSI est un modèle conceptuel subdivisé en sept couches :

3.2.1. La couche physique :

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1). Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie...),

L'unité d'information typique de cette couche est le bit **[3].**

3.2.2. La couche liaison :

Fournit les moyens fonctionnels et procéduraux nécessaires à l'établissement, au maintien et à la libération des connexions de liaison de données entre entités adjacentes du réseau. Elle détecte et corrige, si possible, les erreurs dues au support physique et signale à la couche réseau les erreurs irrécupérables. Elle supervise le fonctionnement de la transmission et définit la structure syntaxique des messages, la manière d'enchaîner les échanges selon un protocole normalisé ou non. Une connexion de liaison de données est réalisée à l'aide d'une ou plusieurs liaisons physiques entre deux machines adjacentes dans le réseau, donc sans nœud intermédiaire entre elles. A noter que dans ce rapport, nous parlerons de couche MAC (Medium Access Control) **[6]** qui se trouve avec la couche LLC (Link Layer Control) **[7]** l'équivalent de la couche liaison dans le modèle 802 **[8]**.

3.2.3. La couche réseau :

Doit fournir d'une part les moyens de maintenir, et de libérer des connexions entre les systèmes ouverts d'autre part de donner les moyens fonctionnels et les procédures nécessaires pour échanger des données entre les entités de transport et les unités du service réseau. Elle a pour but l'envoi de paquets (ensemble structuré de bits) et doit assurer une indépendance vis-à-vis du réseau de communication utilisé (commutation par paquets). Elle doit établir, maintenir et rompre la connexion. Ses principales fonctions sont :

- le routage à travers un réseau pour deux entités non connectées directement (point à point, multipoint ou par diffusion *broadcast*) ;

- assurer le contrôle de trafic (contrôle de flux, contrôle de congestion, etc.) ;

- assurer le contrôle d'erreur (que faire si un nœud du réseau tombe en panne; comment garantir que le réseau ne perdra aucun paquet ?).

Cette couche inclut le puissant protocole Internet (IP, Internet Protocol), le protocole ARP (Adresse Résolution Protocol, protocole de résolution d'adresse) et le protocole ICMP (Internet Control Message Protocol, protocole de message de contrôle Internet) **[3].**

3.2.4. La couche transport :

Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant

que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux.

Cette couche est également responsable de l'optimisation des ressources du réseau : en toute rigueur, la couche transport crée une connexion réseau par connexion de transport requise par la couche session, mais cette couche est capable de créer plusieurs connexions réseau par processus de la couche session pour répartir les données, par exemple pour améliorer le débit. A l'inverse, cette couche est capable d'utiliser une seule connexion réseau pour transporter plusieurs messages à la fois grâce au multiplexage. Dans tous les cas, tout ceci doit être transparent pour la couche session.

Cette couche chargé de fournir un moyen de communication de bout en bout entre 2 programmes d'application. Agi en mode connecté et en mode non connecté. Elle divise le flux de données venant des applications en paquets, transmis avec l'adresse destination IP au niveau IP.

Un des tout derniers rôles à évoquer est le contrôle de flux.

C'est l'une des couches les plus importantes, car c'est elle qui fournit le service de base à l'utilisateur, et c'est par ailleurs elle qui gère l'ensemble du processus de connexion, avec toutes les contraintes qui y sont liées.

L'unité d'information de la couche transport est le message.

Les protocoles de la couche transport à ce niveau sont TCP (Transmission Control Protocol, protocole de contrôle de la transmission), UDP (User Datagram Protocol, protocole de datagramme utilisateur) et SCTP (Stream Control Transmission Protocol, protocole de transmission de contrôle de flux). TCP et SCTP assurent des services de bout en bout fiables. UDP assure des services de datagramme peu fiables [3].

3.2.5. La couche session :

Le rôle de cette couche est de fournir aux entités de présentation les moyens nécessaires pour organiser et synchroniser leur dialogue. Pour arriver à ce but, la couche session doit fournir les services nécessaires à l'établissement d'une connexion son maintien et de ca libération [3].

3.2.6. La couche présentation :

Permet de transcrire les données dans un format compréhensible par les deux systèmes. Elle assure, entre autre, le codage des données dans une norme réseau reconnue et le cryptage éventuel des données **[3].**

3.2.7. La couche application :

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple (le transfert de fichier, la messagerie...).

Ces services fonctionnent conjointement avec la couche transport pour assurer l'envoi et la réception de données. Il existe de nombreux protocoles de couche d'application (http, FTP, et SMTP) **[3].**

4. Le réseau sans fil :

4.1. Définition:

Un réseau sans fil (en anglais Wireless network) **[9][10][11]** est comme son nom l'indique un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fil, un utilisateur à la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité" **[12].**

Les réseaux sans fil sont basés sur une liaison utilisant des ondes radioélectriques (radio et infrarouges) ou des ondes lumineuses. Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée, ainsi que le débit et la portée des transmissions.

Les réseaux sans fil permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres. De plus l'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes comme c'est le cas avec les réseaux filaires (creusement de tranchées pour acheminer les câbles, équipements des bâtiments en câblage, goulottes et connecteurs), ce qui a valu un développement rapide de ce type de technologies.

Ils sont en pleine expansion du fait de la flexibilité de leur interface, ce qui permet à l'utilisateur de changer de place tout en restant connecté.

4.2. Caractéristiques d'un environnement sans fil:

4.2.1. Le bruit :

Le bruit radioélectrique regroupe l'ensemble des signaux ne transportant pas d'information utile et venant perturber le signal désiré, il est donc indépendant du signal émis .il s'agit d'une perturbation aléatoire dont les origines sont le milieu de transmission (bruit externe) et les dispositifs utilisés dans le récepteur (bruit interne) **[13] [14]**.

Les sources de bruit externe peut être d'origine extra-terrestre ou terrestre .elles regroupent les bruits et des parasites atmosphériques, les rayonnements divers captés par l'antenne, les inters errances éventuelles entre les utilisateurs du milieu de transmission ou encore les bruits d'origine industriel. L'effet de ce bruit va dégrader la qualité de transmission sans fil, et engendrer de temps en temps des erreurs de transmission. Ces erreurs causeront par la suite des pertes de paquets .le bruit interne a pour origine le mouvement brownien les électrons étant présents dans les composants électroniques du récepteur .ces électrons étant présente dans la matière en très grand nombre et évoluant indépendamment les uns des autres tout en suivant une même loi, le bruit interne peut alors être modélisé, d'après le théorème de la limite centrale **[15]**, par un processus gaussien.

Toutes les contributions du bruit interne et externe seront prises en compte dans une source unique de bruit n(t) située en amont de récepteur .néanmoins, le bruit interne est en général celui qui est prépondérant dans le système de transmission .par conséquent, lorsque des systèmes a antennes multiples sont étudies, on peut judicieusement supposer que les bruits propres à chacune des antennes sont décarrelés d'une antenne à l'autre et au cours du temps.

4.2.2. La mobilité :

La gestion de mobilité a été largement définie en tant qu'un des problèmes les plus importants pour un accès continu aux réseaux sans fil et aux services mobiles. C'est la technologie fondamentale qui permet aux utilisateurs de terminaux mobiles d'accéder à leurs services tout en se déplaçant et sans rupture de communication. Deux aspects principaux doivent être considérés dans une approche de gestion de mobilité. La gestion de la localisation (adressage, enregistrement et mise à jour de la localisation, paging…) et la gestion du handoff (initiation et déclenchement du handoff…) **[12]**.

5. Caractéristiques du réseau sans fil :

5.1 Puissance du signal :

RSSI (soit Received Signal Strength Indicator, en anglais) est le nom de la force de signal de l'environnement d'un réseau sans fil. Il n'est pas remarquable par l'utilisateur d'un dispositif receveur. Cependant, les dispositifs IEEE 802.11 fournissent à leurs utilisateurs des données de mesure du signal, car la force du signal peut varier de manière considérable, affectant ainsi la fonctionnalité au sein du réseau sans fil.

Les mesures RSSI représentent la qualité relative d'un signal reçu sur un dispositif. RSSI indique le niveau de puissance reçu après une possible perte au niveau de l'antenne et du câble. Plus la valeur RSSI est élevée, plus le signal n'est fort. Lorsque mesuré avec des chiffres négatifs, si le chiffre est proche de zéro ceci signifie qu'il existe un meilleur signal. Par exemple : -50 est un assez bon signal, -75 est un signal plutôt raisonnable et -100 n'est pas un signal du tout .
Même si RSSI et dBm sont des unités de mesure différentes, elles indiquent la force du signal. Le dBm est un taux de puissance de la puissance mesurée en tant que références à un mW (milliwatt). Alors que dBm est un indice absolu, le RSSI est un indice relatif. Pour mesurer de manière significative la bonne qualité d'un signal, il est nécessaire de supprimer le bruit sur la ligne de la puissance du signal. Une différence plus importante du signal par rapport au bruit détermine une meilleure force du signal **[16].**

5.2. Effet du doppler :

Lorsqu'un émetteur et un récepteur se déplacent l'un par rapport à l'autre, la fréquence du signal reçu ne sera pas la même que celle du signal émis. Par exemple, lorsqu' ils se déplacent l'un vers l'autre, la fréquence du signal reçu est supérieure à celle du signal émis. C'est ce qu'on appelle l'effet Doppler. La variation de fréquence due à 1'effet Doppler dépend du mouvement relatif entre la source et le récepteur et de la vitesse de propagation de 1'onde **[17].**

5.3. Problème des nœuds cachés :

Le problème du nœud caché se produit lorsque deux unités mobiles ne peuvent pas s'entendre l'une et l'autre du fait qu'un obstacle les empêche de communiquer entre elles ou que la distance qui les sépare est trop grande **[18].**

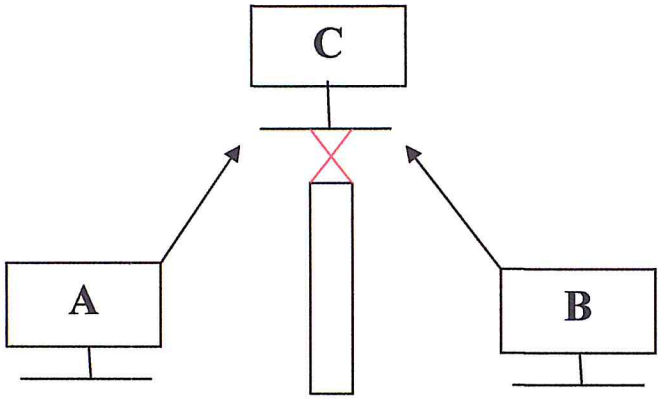

Figure 3 : le phénomène des nœuds cachés

5.4. Problème des nœuds exposés :

Considérons le cas présenté en Figure 4 où on suppose que les stations A et C sont dans le rayon de porté de la station B, et la station A est hors du rayon de porté de la station C.

On suppose aussi que la station B elle est entrain de transmettre à la station A, et la station C a une trame à transmette vers la station D. Selon le mécanisme de détection de porteuse, le lien de la station C devient un canal occupé en raison des transmissions de la station B. Par conséquent, la station C ne peut pas transmettre à D, même si cette transmission ne crée pas une collision dans les régions où *D* et *A* se situent. Ce problème diminue les performances du réseau en termes de bande passante. **[18]**

Figure 4 : le phénomene des nœuds exposés

5.5. Contraintes d'énergie :

Les applications relatives aux réseaux sans fil ont en général un caractère normal et tirent leur autonomie de batterie .émettre ou recevoir des données consume de l'énergie et l'on peut chercher à l'économiser en optimisant les protocoles de gestion du réseau .la puissance d'émission a un impact important sur la quantité d'énergie utilisée et là encore on essaie si possible de la limiter à ce qui est strictement nécessaire **[19].**

5.6. Congestion : La congestion est la condition dans laquelle le paquet bloqué quelque part dans le réseau ce qui retardé le paquet à arriver à la destination. C'est le moment où

l'augmentation du trafic (flux) provoque un ralentissement. Les trames entrantes dans les buffers des commutateurs sont rejetées dans ce cas puisque le buffer est saturé, qu'il ne peut plus stocker de nouveaux paquets et qu'il y a par conséquent une perte de paquets **[58].**

6. Type de réseaux sans fil :

Les réseaux sans fil peuvent avoir une classification selon deux critères. Le premier est la zone de couverture du réseau. Au vu de ce critère il existe quatre catégories : les réseaux personnels, les réseaux locaux, le réseau métropolitain et les réseaux étendus. Le second critère est l'infrastructure ainsi que le modèle adopté. Par rapport à ce critère on peut diviser les réseaux sans fils en : réseaux avec infrastructures et réseaux sans infrastructure, comme on le voit dans l'illustration de la figure suivante

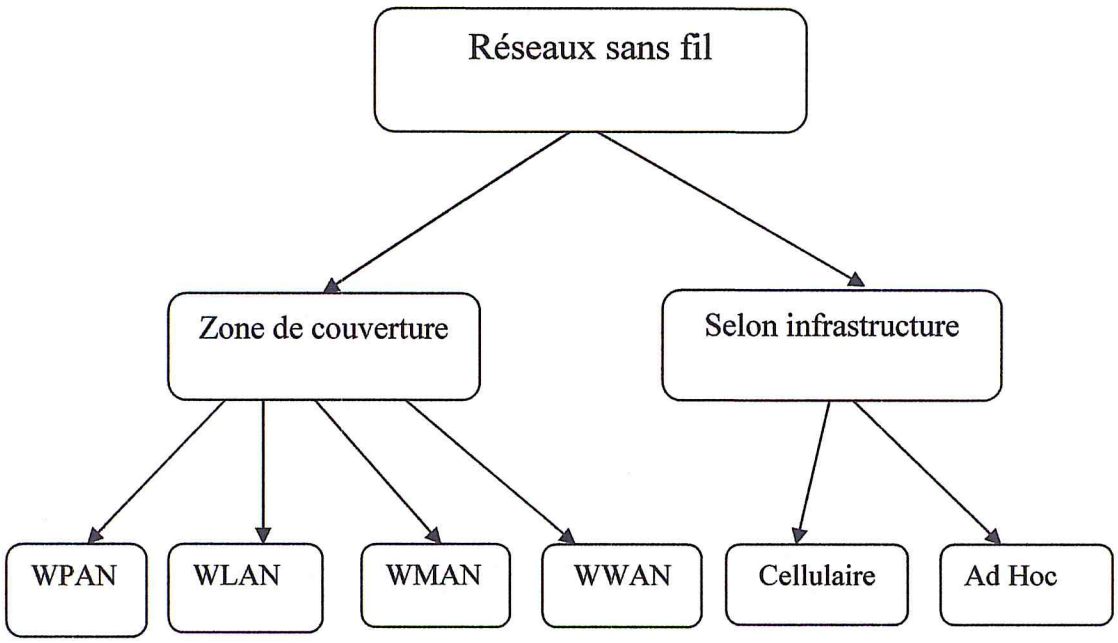

Figure 5: Classification des réseaux sans fil.

6.1. Classification des réseaux en fonction de la portée :

On distingue habituellement plusieurs catégories de réseaux sans fil **[20][12]**selon le périmètre géographique offrant une connectivité (appelé Zone de couverture). Ces technologies peuvent être classées en quatre parties :

6.1.1 Les réseaux personnels sans fil : WPAN (Wireless Personal Area Network) : **[20]** appelé également réseau individuel sans fil ou réseau domestique sans fil, concerne les réseaux sans fil d'une faible portée : de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils

domestiques, ...) ou un PDA (Personal Digital Assistants) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes. On y trouve le standard tel que le Bluetooth.

A. Le Bluetooth : Nom commercial de la norme IEEE 802.15.1, Bluetooth **[21] [22]** est Aujourd'hui présent dans de nombreux dispositifs. Malgré un débit de 1 Mb/s et une portée d'environ 30 mètres, Bluetooth offre de nombreuses possibilités grâce à la faible consommation de ses équipements. On trouve des composants Bluetooth dans beaucoup d'ordinateurs portables mais aussi dans de nombreux périphériques (appareils photo, téléphones portables, assistants personnels, ...). La norme IEEE 802.15.3 (Bluetooth2) est une évolution de la norme Bluetooth permettant des débits plus rapides et intégrants des mécanismes de sécurité très limités dans le protocole Bluetooth.

6.1.2. Les réseaux locaux sans fil : WLAN (Wireless Local Area Network) : **[23]** C'est la catégorie des réseaux locaux sans fil dont la portée va jusqu'à 500 m, pour les applications couvrant un campus, un bâtiment, un aéroport, un hôpital, etc. Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet). La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbit/s (pour un réseau Ethernet par exemple) et 1 Gbit/s (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.

On y trouve le standard tel que le Wi-Fi (Wireless Fidelity) .

A. Le WiFi (Wireless Fidelity):

Le Wifi (Wireless Fidelity) **[24]** (ou IEEE 802.11b), soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) **[25]** offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres. La particularité du phénomène WiFi, devenant progressivement aussi célèbre que le web, est que des micro-réseaux, se développent de proche en proche dans les quartiers et les villes formant ainsi une toile sans fil interconnectant à haut débit des ordinateurs, des PDAs, des pocketPCs et des téléphones portables. Le standard WiFi 802.11b offre un débit élevés sont proposés par ses successeurs parmi lesquels on trouve les standards IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n et IEEE 802.11ac.

6.1.3. Les réseaux métropolitains sans fil : WMAN (Wireless Metropolitan Area Network) **[26]** : Interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un WMAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local. Un WMAN est formée de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique). C'est dans cette catégorie que l'on classe le WiMAX .

A. Le WiMAX :

Le WiMAX ou World wid. Inter operability for Micro wave Access 8**[27]** est une famille de normes, définissant des connexions à haut-débit par voie hertzienne, développée par le Consortium WiMAX Forum et ratifié en 2001 par l'IEEE sous le nom IEEE-802.16. Le WiMAX est aussi le nom commercial délivré par le WiMAX Forum aux équipements conformes à la norme IEEE 802.16, afin de garantir un haut niveau d'interopérabilité entre ces différents équipements.

6.1.4 Les larges réseaux sans fil : WWAN (Wireless Wide Area Network) **[26]**:

Également connu sous le nom de réseau cellulaire mobile, sont les réseaux sans fil les plus Répandus puisque tous les téléphones mobiles sont connectés à un de ces réseaux étendus.

Interconnecte plusieurs LANs à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet.

Dans cette catégorie, on peut citer le GSM et ses évolutions GPRS.

A. GSM (General Packet Radio Service) **[28] :** Le GSM est un système de radiotéléphonie cellulaire numérique, qui offre à ses abonnés des services qui permettent la communication de station mobile de bout en bout à travers le réseau. La téléphonie est le service le plus important des services offerts. Ce réseau permet la communication entre deux postes mobiles ou entre un poste mobile et un poste fixe. Les autres services proposés sont la transmission de données et la transmission de messages alphanumériques courts.

B. GPRS (General Packet Radio Service) **[29] :** est une norme pour la téléphonie mobile dérivée du GSM permettant un débit de données plus élevé. On le qualifie souvent de 2,5G.

Le G est l'abréviation de génération et le 2,5 indique que c'est une technologie à mi-chemin entre le GSM (2eme génération) et l'UMTS (3eme génération).

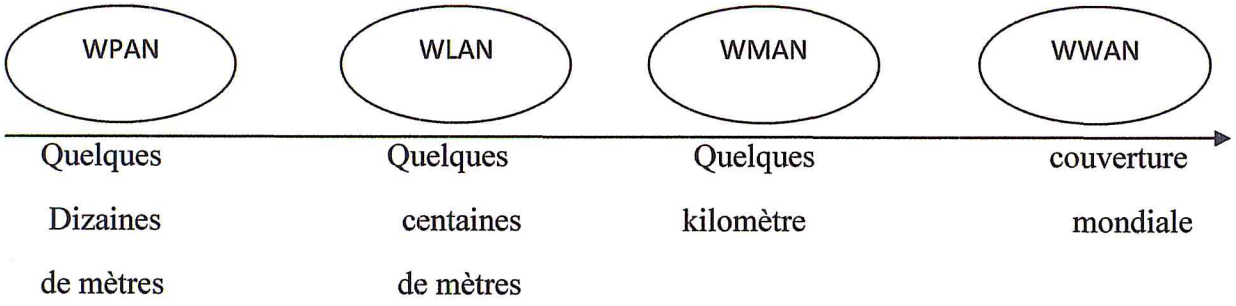

Figure 6: Classification des réseaux sans fil suivant leur taille

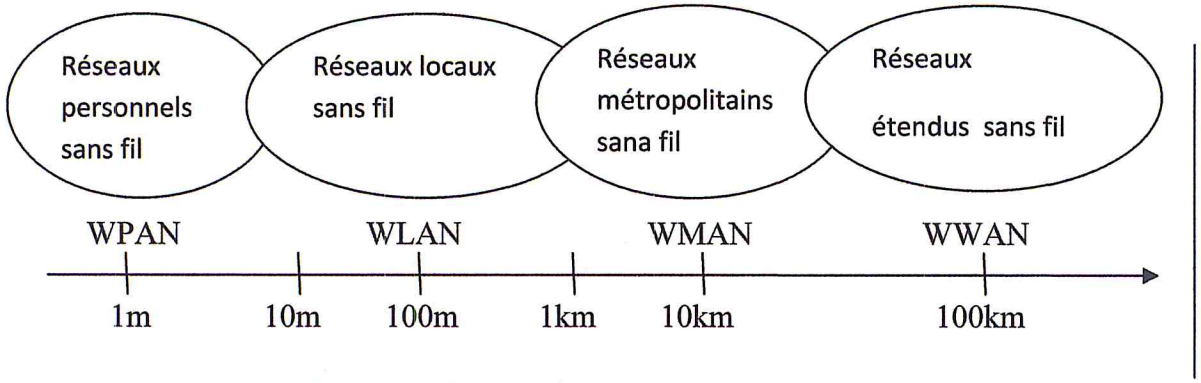

Figure 7: Les différentes technologies sans fil.

6.2. Classification des réseaux suivant le mode opératoire :

6.2.1. Le mode infrastructure :

En mode infrastructure, le réseau est composé de plusieurs cellules, chacune d'elles comprend une station de base (ou un point d'accès) par laquelle toutes les autres stations de la cellule accèdent au réseau intra et intercellulaire. Les différents points d'accès sont reliés entre eux et/ou au réseau Internet à l'aide d'une technologie supplémentaire qui peut être filaire ou hertzienne. Dans cette catégorie, on trouve les réseaux WLAN (Wi-Fi), WMAN (WiMAX) et WWAN (GSM)**[30]**.la [Figure 8]représente l'architecture de mode infrastructure

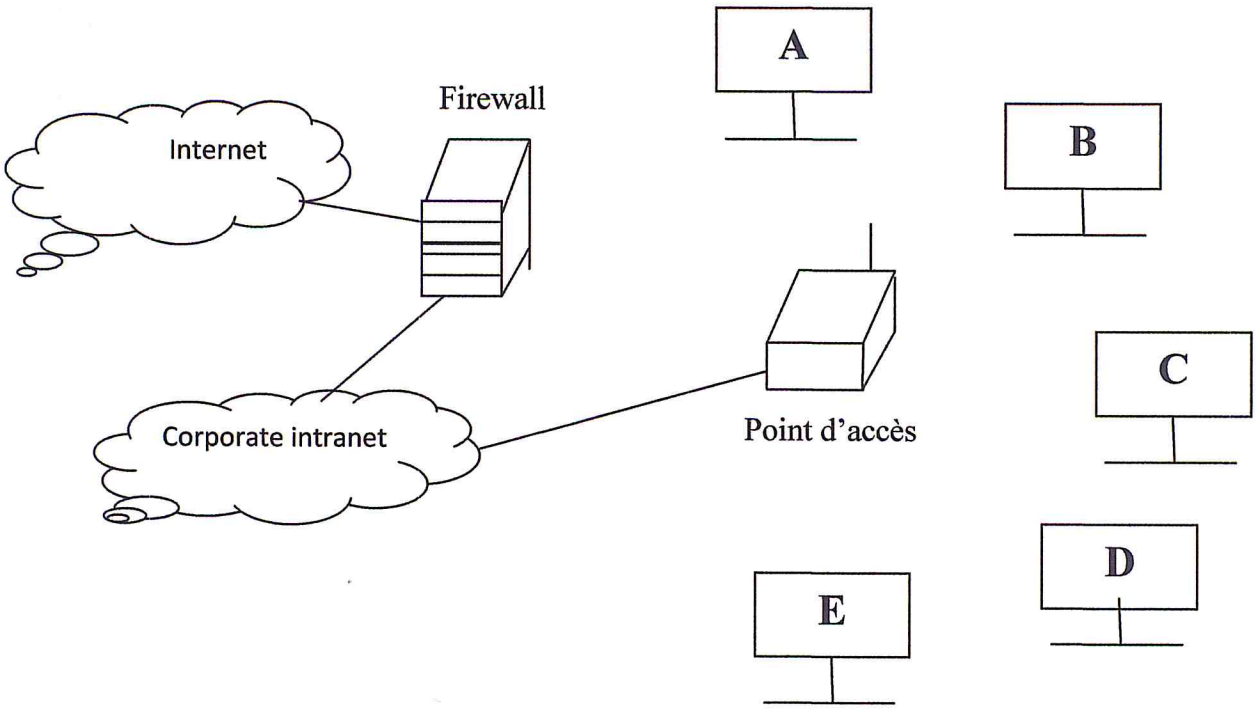

Figure 8: architecture de mode infrastructure

6.2.2. Le mode sans infrastructure (Ad hoc) :

En mode ad hoc, il n'y a pas de point d'accès fixe, l'infrastructure n'est composée que des stations elles-mêmes, ces dernières jouant à la fois le rôle de terminaux et de routeurs pour permettre le passage de l'information d'un terminal vers un autre sans que ces terminaux soient reliés directement. La caractéristique essentielle d'un réseau ad-hoc est l'existence de tables de routage dynamiques dans chaque nœud. C'est la catégorie des réseaux WPAN tels que le Bluetooth **[31]**. La **[Figure 9]** représente l'architecture de mode sans infrastructure

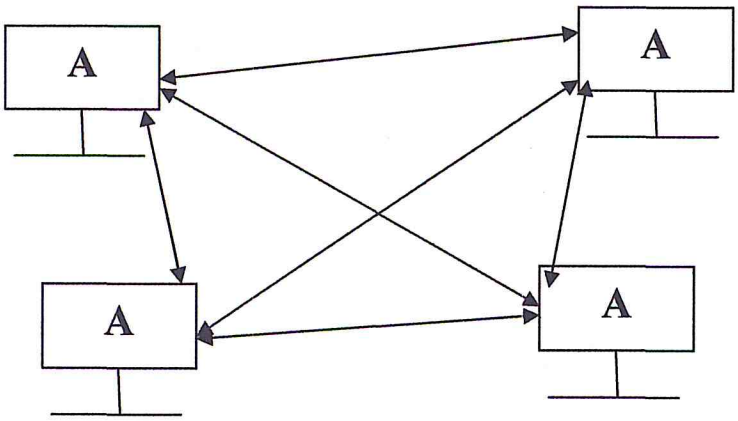

Figure 9 : architecture de mode sans infrastructure

6.3. Comparaison Les réseaux ad hoc et les réseaux cellulaires :

Le **Tableau 1** donne les principales différences entre les réseaux ad hoc et les réseaux cellulaires :

Les réseaux cellulaires	Les réseaux ad hoc
Des réseaux avec infrastructure	Des réseaux sans infrastructure
Les sites des stations de base fixe sont pré-localisés.	N'est pas de station de base
Topologie de réseau statique	Topologie de réseau très dynamique avec multi-sauts
Environnement relativement occupé et une connectivité stable	Environnement hostile (bruit, pertes) et une connectivité irrégulière
Une planification détaillée avant l'installation de la station de base	Un réseau ad hoc qui se forme automatiquement et s'adapte aux changements
Les coûts d'installation élevés	Moins coûteuse
Nécessite beaucoup de temps pour l'installation	rapidité d'installation

Tableau 1 : comparaison entre les réseaux cellulaires et les réseaux ad hoc.

7. Le protocole TCP :

7.1. Définition de protocole TCP :

Le protocole de contrôle de transmission TCP a été défini pour fournir un service de transfert de données fiable entre deux applications sur des stations distantes raccordées par un réseau à commutation de paquets utilisant le protocole IP (Internet Protocol). La fiabilité du transfert est obtenue par différents mécanismes tels que l'établissement de connexion, la gestion de timers de retransmissions ou encore le contrôle de la fenêtre de retransmissions. La spécification initiale, définie dans le Request For Comments RFC 793 de 1981 a fait l'objet de nombreux travaux qui ont conduit à des améliorations de la spécification initiale.

Dans la pratique, la plupart des déploiements du protocole TCP ont été soigneusement conçus dans le contexte des réseaux câblés. Dans un environnement ad hoc l'implémentation de TCP peut conduire à des performances médiocres dues aux propriétés intrinsèques des réseaux sans fil [32].

7.2. Structuration de données TCP : La figure suivante donne la structure d'un segment TCP.

L'en-tête d'un segment se compose des champs suivant **[37] :**

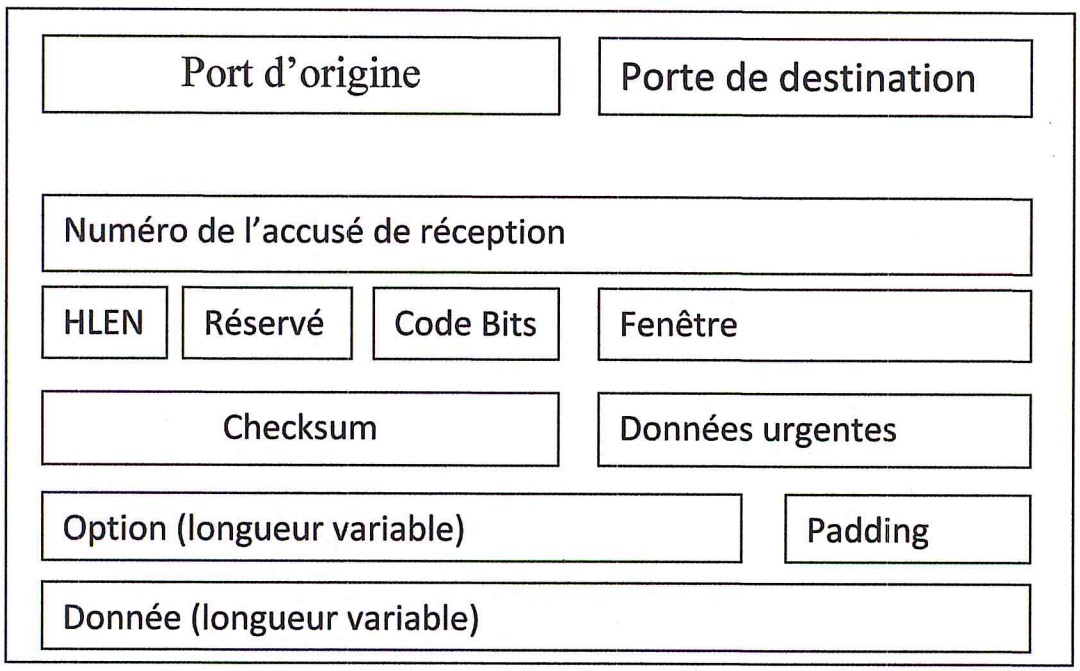

Figure 10: Format d'un message TCP

– **Numéros de port** : indiquent les ports associés à la connexion (entiers de 16 bits). Plusieurs ports sont réservés pour des applications courantes (20 et 21 : FTP; 23 : Telnet; 25 : SMTP; 53 : DNS; 80 : HTTP; 110 : POP3).

– **Numéro de séquence du premier octet du segment** est indiqué dans l'en-tête du message afin que la destination puisse reconstituer les données originales.

– **Numéro d'accusé de réception** : est le numéro du prochain octet attendu par l'émetteur de l'acquittement (il acquitte ainsi implicitement les octets portant un numéro inférieur).

-**Champ « Réservé »**: qui se trouve dans l'en-tête de segment TCP. A l'origine ce champ a été réservé pour un usage futur.

– **HLEN (Header Length)** : contient la longueur de l'entête TCP (en mots de 32 bits).

– **Code Bits** : indique la nature du segment. Ces bits sont :

–**URG:** le pointeur de données urgentes est valide. Les données sont alors transmises sans délai et les données remises sans délai à la réception.

–**SYN:** utilisé à l'initialisation de la connexion pour indiquer où la numérotation séquentielle (numéro de séquence) débute. Le Numéro de séquence inscrit dans un datagramme SYN est le Initial Sequence Number (ISN) produit par un générateur garantissant l'unicité de l'ISN sur le réseau (indispensable pour identifier et éliminer les doublons).

–**FIN:** utilisé lors de la fermeture normale de la connexion.

–**PSH (push) :** en émission, TCP reçoit les données depuis l'application, les transforme en segments à sa guise puis les expédie. Une entité TCP décodant le bit PSH, transmettra les données sans attendre plus longtemps. A la réception, elles seront immédiatement transmises au niveau supérieur. Par exemple, en émulation de terminal, on veut que chaque caractère soit envoyé (mode caractère asynchrone). On utilise donc PSH.

–**RST:** utilisé par une extrémité pour indiquer à l'autre extrémité qu'elle doit réinitialiser la connexion. Ceci est utilisé lorsque les extrémités sont désynchronisées.

–**Fenêtre :** indique la quantité de données que l'émetteur de ce segment accepte de recevoir. Ceci est mentionné dans chaque message. C'est une façon de contrôler le flux des données.

–**Checksum :** calcul du champ de contrôle. Utilise un pseudo en tête dans son calcul et s'applique à la totalité du segment obtenu.

–**Options :** permet de négocier la taille maximale des segments échangés. Ce champ n'est présent que dans les segments d'initialisation de connexion (avec bit SYN).

7.3. Caractéristiques du TCP:TCP est bien compliqué qu'UDP, il apporte en contrepartie des services beaucoup plus élaborés. Sept principaux caractérisent le TCP **[33]**:

7.3.1. Orienté connexion : signifie que deux machines souhaitant communiquer via TCP doivent commencer par établir une connexion avant de pouvoir dialoguer. Une fois la connexion établie, les deux extrémités de la connexion peuvent communiquer de manière bidirectionnelle (full-duplex).

7.3.2. La fiabilité : il utilise des mécanismes d'acquittement, de retransmission de paquets ainsi que des timers afin délivrer de bout en bout les données avec la plus haute fiabilité.

7.3.3. L'ordre : il assure que les paquets arrivent dans le même ordre que celui d'émission en utilisant à la fois des numéros de séquence de paquets et des tampons de réception.

7.3.4. Le contrôle de congestion : des mécanismes de contrôle de congestion **[34]** (Slow-Start, Congestion Avoidance, Fast Retransmit, Fast Recovery) permettent d'éviter l'engorgement du réseau lorsque ce dernier est saturé et d'augmenter le débit de transmission lorsque le réseau est faiblement chargé.

7.3.5. Le contrôle de flux : TCP fournit un mécanisme de fenêtre d'émission glissante dynamique pour contrôler le débit de transmission de l'émetteur. Ce dernier ne peut émettre plus rapidement que le récepteur l'autorise. Ce mécanisme est également utilisé pour le contrôle de congestion.

7.3.6. Transfert de flux d'octets de données : TCP découpe les flux d'octets de données de l'application en segments dont la taille est déterminée par le mécanisme de fenêtre glissante.

7.3.7. Contrôle d'erreur sur bit : TCP intègre un mécanisme de checksum sur 16 bits pour couvrir les erreurs sur bit de l'entête et des données.

7.4. Fonctionnement général du protocole TCP :

7.4.1. Ouverture d'une connexion TCP : L'établissement d'une connexion TCP s'effectue en trois étapes (voir la figure 11) **[32]**:

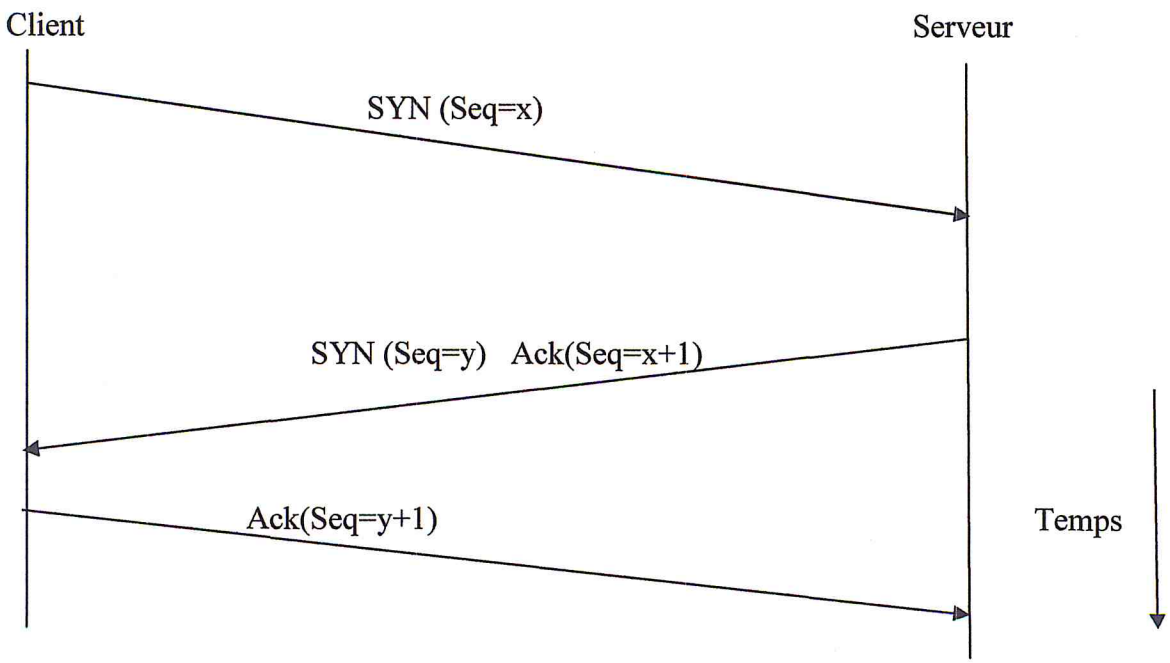

Figure 11: Ouverture d'une connexion TCP

a. Le client envoie un segment comportant le drapeau SYN, avec sa séquence initiale (ISN = x).

b. Le serveur répond avec sa propre séquence (ISN = y), mais il doit également acquitter le paquet précédent, ce qu'il fait avec ACK (Seq = x + 1).

c. Le client doit acquitter le deuxième segment avec ACK (Seq = y + 1).

Une fois achevée cette phase nommée 'THREE WAY HANDSHAKE', les deux applications sont en mesure d'échanger les octets qui justifient l'établissement de la connexion.

7.4.2. Le mécanisme de l'acquittement :

La mise en œuvre de la fiabilité passe par l'utilisation de paquets d'acquittement (ACK) et de numéros de séquences (conceptuellement le numéro du premier octet contenu dans un paquet). Lorsqu'un nœud reçoit un paquet, il émet un acquittement en renseignant le numéro de séquence jusqu'auquel il a reçu tous les octets. On parle d'acquittement cumulatif. Il est alors possible que l'on obtienne un second acquittement pour un même numéro de séquence (acquittement dupliqué), qui signifie qu'un paquet précédent a été détruit dans le réseau ou qu'il y est retardé. Dans ce cas, TCP doit réémettre le paquet en question avant l'expiration du délai de retransmission, le RTO, propre à chaque paquet (RTO).

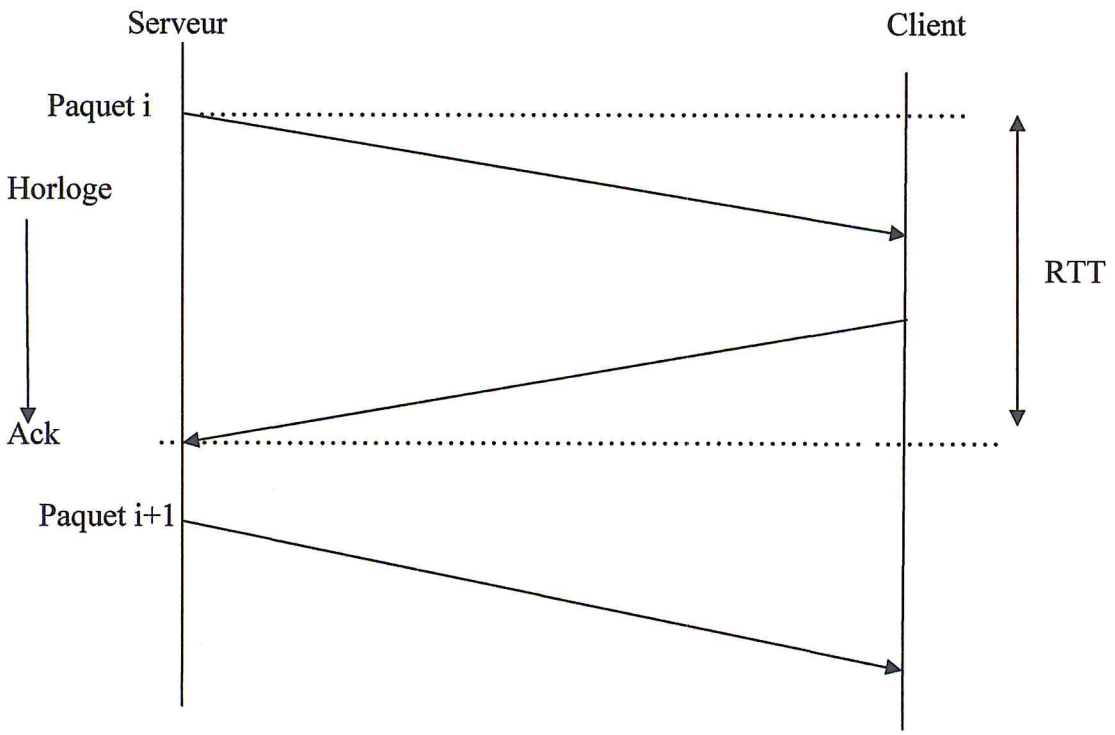

Figure 12: Mécanisme de l'acquittement

Le RTO, est calculé à partir du temps de transmission aller-retour (RTT) *[35].*

7.4.3. La fermeture d'une connexion TCP : Un échange de trois segments est nécessaire pour l'établissement de la connexion **[32]**, il en faut quatre pour qu'elle s'achève de manière canonique ' ORDERLY RELEASE'. La figure 13 décrit le mécanisme de fermeture d'une connexion TCP

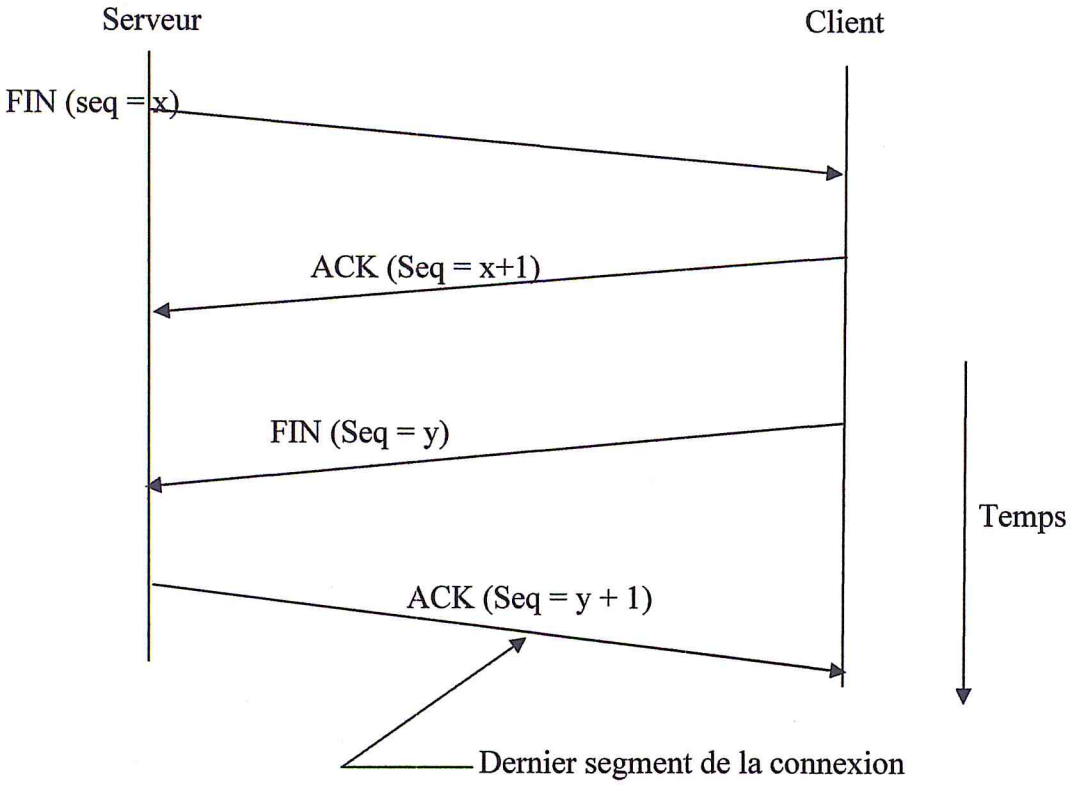

Figure 13 : Fermeture de connexion TCP

Dans l'établissement d'une fermeture de connexion TCP, L'application qui envoie un paquet avec le drapeau FIN indique à la couche TCP de la machine distante qu'elle n'enverra plus de donnée. La machine distante doit acquitter ce segment, comme il est indiqué sur la figure, en incrémentant d'une unité le "Sequence Number". La connexion est véritablement terminée quand les deux applications ont effectué ce travail. Il y a donc échange de 4 paquets pour terminer la connexion.

Au total, sans compter les échanges propres au transfert des données, les deux couches TCP doivent gérer 7 paquets.

7.5. Fonctions de contrôle de congestion : Le contrôle de congestion est un mécanisme qui permet de régir le débit d'un ou de plusieurs flux. Ce mécanisme vise généralement à répondre aux trois exigences suivantes : **[36]**

- Maximiser l'utilisation de la bande passante.

- Limiter le nombre de paquets perdus, c'est-à-dire ne pas dépasser les capacités des ressources du réseau.

- Partager équitablement la bande passante entre les différents flux parcourant le ou les liens les plus lents.

TCP régule ses envois à travers un système de fenêtre glissante (sliding window) qui définit la quantité de paquets pouvant être envoyés sans être acquittés, en termes de numéro de séquence. Cette fenêtre, dite fenêtre de transmission, que l'on abrègera en TWND, est calculée à partir de deux autres fenêtres.

a. La fenêtre permise, notée Rcvwnd. permet au récepteur d'annoncer le nombre de segments qu'il est capable actuellement de recevoir.

L'envoi de cette valeur dans chaque paquet constitue le contrôle de flux.

b. La fenêtre de congestion, notée Cwnd. Celle-ci est maintenue par le contrôle de la congestion qui s'effectue au niveau de l'émetteur.

La fenêtre de transmission est alors régie par la formule : Min (Cwnd, Rcvwnd)

7.5.1. Slow Start (démarrage lent) :

La réaction du TCP à un acquittement manquant est tout à fait efficace, mais il est nécessaire de se débarrasser de la congestion rapidement. Le comportement du TCP déclenché après la détection de la congestion est appelé « démarrage lent » **[37]**.

L'expéditeur toujours calcule la fenêtre de congestion pour un récepteur. La taille de démarrage de la fenêtre de congestion est d'un segment (paquet TCP). L'expéditeur envoie un paquet et attend un acquittement. Si cet acquittement arrive, il incrémente la fenêtre de congestion par un autre segment. Puis il envoie deux paquet (fenêtre de congestion = 2). Après l'arrivé de deux acquittements correspondants, l'expéditeur ajoute une autre fois deux à la fenêtre de congestion (un pour chaque acquittement). Donc la fenêtre de congestion deviendra quatre. Ce schéma consiste à doubler la fenêtre congestion à chaque réception des acquittements, qui prennent un temps d'aller-retour (RTT). Ceci s'appel la croissance exponentielle de la fenêtre de congestion dans le mécanisme du démarrage lent.

L'incrémentation linéaire continue jusqu'à l'expiration du temps au niveau de l'expéditeur à cause d'un acquittement manquant, ou jusqu'à la réception d'un acquittement dupliqué pour le même paquet. Dans les deux cas TCP quitte alors la phase de slow-start pour passer en mode d'évitement de congestion et divise par deux la fenêtre de congestion.

7.5.2. Congestion avoidance [38] :

Au-delà d'une certaine limite de valeur de cwnd (slow start threshold, ssthresh), TCP passe en mode d'évitement de congestion. À partir de là, la valeur de cwnd augmente de façon linéaire et donc bien plus lentement qu'en slow start : cwnd s'incrémente de un MSS (= un paquet) à chaque RTT. Dans ce mode de fonctionnement, l'algorithme détecte aussi rapidement que possible la perte d'un paquet : si nous recevons trois fois l'ACK même paquet, on n'attend pas la fin d'un timeout pour réagir. En réaction à cette perte, on fait descendre la valeur de ssthresh ainsi que cwnd (on repasse éventuellement en mode de Slow Start). On utilise la technique de Fast Retransmit pour renvoyer rapidement les paquets perdus.

7.5.3. L'algorithme Additive Increase and Multiplicative Decrease (AIMD):

TCP utilise l'algorithme distribué Additive Increase and Multiplicative Decrease (AIMD) **[39] [40]** permettant de faire converger les différents flux partageant les mêmes conditions réseaux vers le même débit équitable. Cet algorithme est basé sur une augmentation additive assuré par la phase d'évitement de congestion et une réduction multiplicative de la fenêtre cwnd réalisée à chaque congestion où cwnd est réduite de moitié.

Lorsque cwnd atteint la taille correspondant à un partage équitable de la bande passante, le même débit est obtenu par chaque flux TCP de même RTT traversant le lien congestionné. Dans ce cas, chaque flux subit les cycles d'une perte suivie d'une phase d'évitement de congestion.

Pour sortir d'une congestion d'autres solutions ont été proposées où la fenêtre de congestion est réduite différemment. Les objectifs à garder en vue pour ces algorithmes sont d'être efficaces, équitables et qu'ils présentent une convergence vers une solution adéquate à partir d'un état quelconque et avec une vitesse assez rapide.

7.6. La reprise sur l'erreur :

7.6.1. Fast retransmit (retransmission rapide) : Cet algorithme est une modification de l'algorithme Congestion avoidance, la détermination d'une perte n'est plus donnée uniquement par l'expiration du temporisateur de retransmission **RTO** mais aussi par ce qu'on appelle les acquittements dupliqués. Expliquons en premier ce que sont les acquittements dupliqués. Lorsqu'un récepteur reçoit une donnée, il envoie un acquittement portant le numéro de la prochaine séquence attendue. Si le dernier segment envoyé se perd ou est en retard, le récepteur accepte les autres segments qui arrivent mais va continuer d'envoyer des acquittements portant ce même numéro de séquence jusqu'à ce qu'il ait reçu le bon segment ou que le temporisateur **RTO** expire. La théorie des acquittements dupliqués soutient qu'au-delà d'un nombre fixé d'acquittements portant le même numéro de séquence, on peut conclure une perte sans attendre que **RTO** expire.

C'est le changement apporté dans fast retransmit où après l'arrivée de (3) acquittements successifs dupliqués (4 acquittements portant le même numéro), TCP enclenche une réinitialisation suite à ce qui parait être la perte d'un message. La fenêtre de congestion cwnd est remise à un (1) et le seuil ssthresh est mis à jour, puis la transmission reprend selon l'algorithme Slow Start. Ce comportement est appelé « Fast Retransmit » **[41]**.

7.6.2. Fast-recovey (recouvrement rapide) :

L'algorithme le plus couramment implémenté dans le TCP est FastRecovery. Celui-ci permet de retrouver rapidement l'état d'équilibre en évitant comme dans les versions précédentes de TCP de passer par l'algorithme Slow Start pour toute réinitialisation suite à des pertes. Cet algorithme est utile lorsque les fenêtres de transmission sont grandes et qu'il n'y a que très peu de pertes par temps de boucle. L'idée ajoutée dans cet algorithme est donc de ne pas reprendre une transmission à Slow Start après une perte détectée par les acquittements dupliqués. La transmission reprend directement avec congestion avoidance. En effet, d'une part, Slow Start est une phase où la transmission n'est pas stable et où la conservation n'est pas encore appliquée.

D'autre part, le fait qu'il y ait des acquittements qui arrivent à l'émetteur signifie que des segments arrivent au récepteur, donc, il se produit peut être des pertes sur la ligne mais celle-ci continue malgré tout de transmettre des messages et il n'est pas nécessaire de diminuer trop brutalement la cadence de la transmission **[36]**.

8. Différentes versions de TCP :

8.1 TCP Tahoe :

V.Jacobson[42] donne les premières améliorations de TCP au niveau de ses algorithmes de contrôle de congestion est TCP Tahoe. C'est la plus simple et la moins efficace (tous types de problème confondus). Cette version utilise un système de slow start, avec une valeur initiale de cwnd à 1 et une valeur de cwnd maximum de ssthresh. La première fois qu'on effectue un slow Start on arrive à une perte de paquet, dans ce cas la valeur de cwnd courante sera notre nouveau ssthresh puis on remet la valeur de cwnd à 1. Une fois ssthresh atteint, on entre en Congestion Avoidance. À partir de là la valeur de cwnd augmente d'une façon linéaire et donc plus lentement qu'en Slow Start. Lorsqu'on reçoit trois fois le même ACK, TCP déduit qu'il y a une congestion, on n'attend pas le timeout avant de renvoyer le paquet perdu (fast retransmit).

Il n'y a pas de FastRecovery, on passe la valeur de ssthresh à la moitié de cwnd courant, cwnd passe à 1MSS et on retourne en Slow.

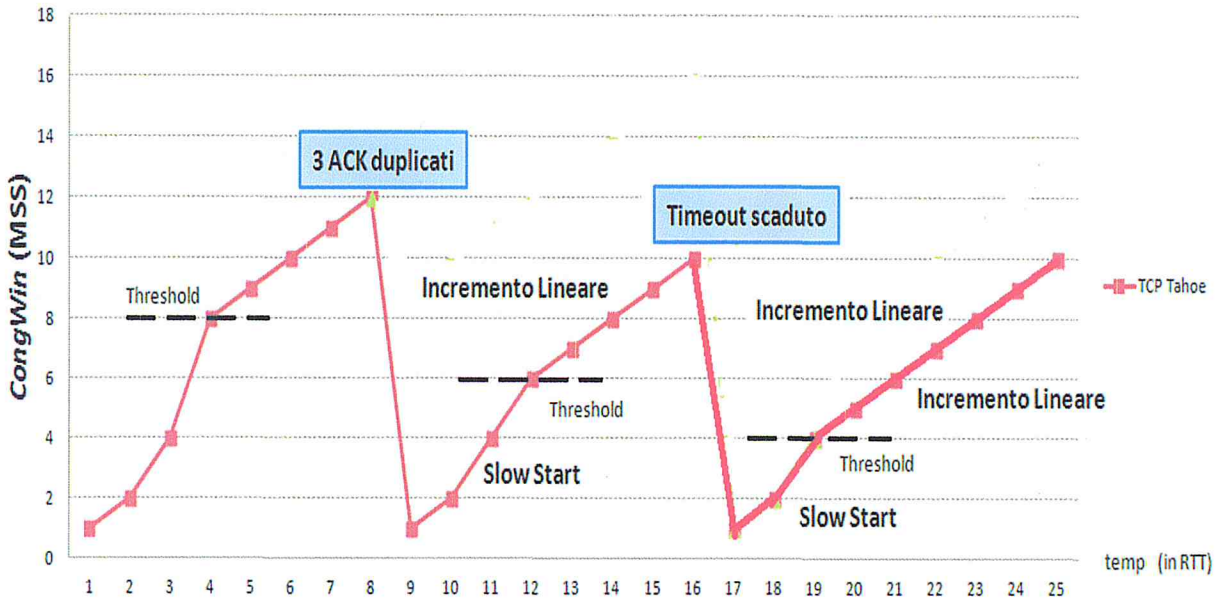

Figure 14: TCP Taheo

8.2 TCP Reno:

Jacobson propose également dans [42] un autre algorithme qui rend la transmission plus efficace. La différence avec Tahoe est qu'il utilise le FastRecovery. Une fois la réception de trois ACK dupliqués on diminue de moitié la valeur de cwnd, on met le seuil de ssthresh à la

taille de cwnd, on fait un fast retransmit et on passe en FastRecovery. Si on a un timeout on repart en Slow Start comme avec Tahoe, avec la fenêtre de congestion à 1MSS.

TCP Reno permet donc de ne pas repartir en Slow Start (et avec un cwnd à 1) dès qu'il y a congestion. Les débits sont donc plus stables.

Cette version garde l'inconvénient d'être peu rapide pour la réémission de données suite à un Time Out à cause d'une granularité peu fine utilisée dans le système d'horloge pour le calcul des RTT **[43].**

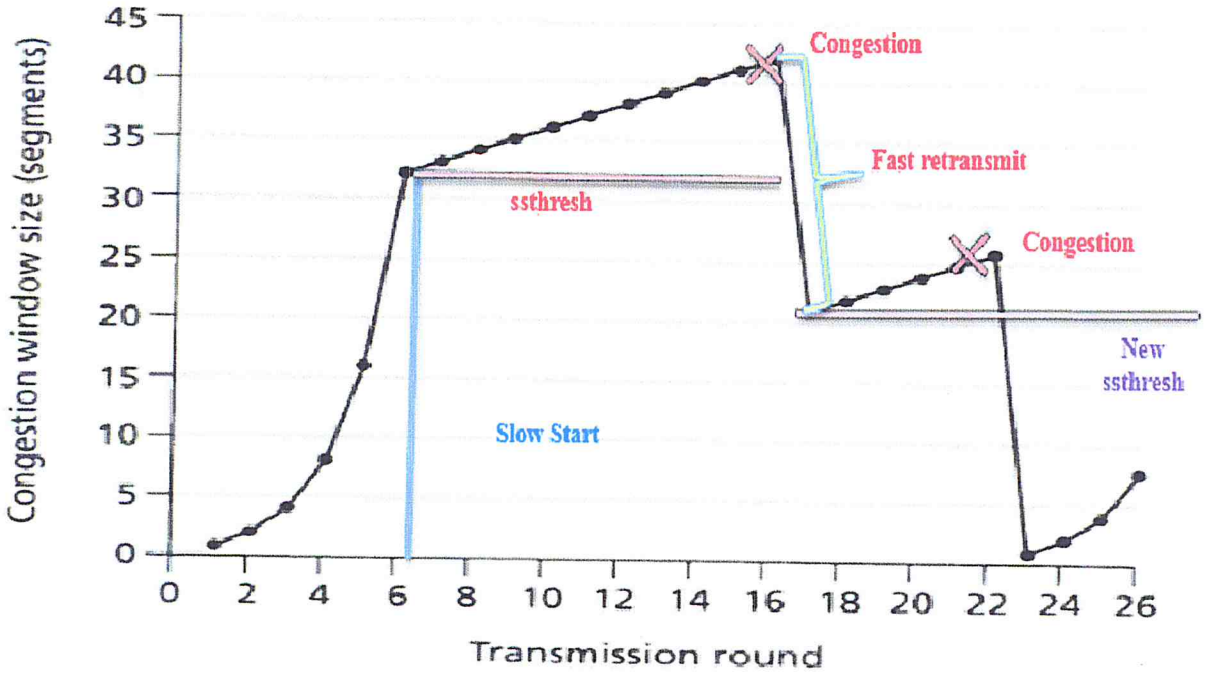

Figure 15: TCP Reno.

8.3 TCP Vegas :

La version de TCP Vegas **[44]** change le procédé par lequel elle fait varier les tailles des fenêtres par rapport aux autres versions de TCP. Plutôt que d'attendre une perte de paquet, TCP Vegas prend en compte le temps de réponse du destinataire (le RTT) afin d'en déduire le ratio auquel envoyer les paquets. En fonction du temps de réponse, on est capable de supposer l'état des buffers des routeurs intermédiaires.

TCP Vegas modifie pour cela plusieurs algorithmes vus jusqu'ici (Slow Start, Congestion avoidance, Fast Retransmit).Grâce à cette technique TCP Vegas à de meilleurs débits et moins

de pertes de paquets que Reno. Cet algorithme permet d'atteindre un partage équitable des ressources. De même, il y a assez peu de pertes avec TCP Vegas puisqu'à l'état stable, le débit correspond de près à la capacité du lien **[45].**

Puisque TCP Vegas permet de s'adapter plus rapidement aux changements de disponibilité du lien, les performances se dégradent lorsqu'il est utilisé avec d'autres protocoles qui ne prennent pas en compte l'état du lien *avant* une perte de paquet. Un inconvénient cependant, il nécessite une modification de la pile TCP pour l'émetteur et le récepteur.

8.4. TCP New Reno :

Cet algorithme s'appelle « NewReno » parce qu'il n'est qu'une modification légère (mais significative) de l'algorithme Reno. En effet, la modification s'opère au niveau de la phase de FastRecovery : on reste dans ce mode tant que nous n'avons pas reçu les ACK de tous les paquets perdus. Lorsqu'il y a une perte de plusieurs segments d'une même « rafale » envoyée, à la réception d'un acquittement partiel on renvoie le segment perdu suivant, sans sortir du mode Congestion avoidance, contrairement à Reno qui sort de ce mode dès la réception d'un ACK non dupliqué **[46].**

La version de TCP New Reno est parmi les versions les plus utilisées de TCP actuellement.

8.5. TCP Sack :

Dans **[47]** est proposée une méthode où est apportée une modification au contenu des accusés de réception.

Les algorithmes de Slow Start et de Congestion avoidance sont les mêmes que pour TCP Reno. Selective ACK TCP permet, lors d'une perte, de dire qu'on a reçu les paquets jusqu'à la séquence numéro N, mais aussi de préciser à l'émetteur qu'on a bien reçu certains des paquets suivant. L'émetteur n'a plus à renvoyer des segments déjà reçus. SACK est une option qui se négocie à la connexion. Cette option permet de gagner un peu de performances, lors de pertes de segments, mais il est nécessaire d'avoir les deux parties (émetteur et récepteur) qui l'implémentent.

9. Les performances du protocole TCP dans les réseaux mobiles ad hoc :

Performances du protocole TCP dans un nœud mobile doit prendre en considération les facteurs suivants :

9.1. Délai de congestion :

L'un des problèmes principaux du TCP est qu'il assigne toutes les pertes de paquet à la congestion, et que ce phénomène de perte est géré par le schéma de contrôle de cogestion. Quand une perte de paquet est détectée, la fenêtre de congestion est réduite, et l'horloge de retransmission est réinitialisée à un intervalle de backoff. Les algorithmes de contrôle de congestion doivent être utilisés seulement en cas d'une véritable congestion du réseau. Notant que V. JACOBSON **[48]** suppose que la perte de paquets endommagés pendant le transport est rare, d'où probablement les paquets sont perdus en raison de la congestion du réseau et non en raison de l'endommagement des paquets. Dans l'algorithme de VAN JACOBSON, on trouve que le schéma de contrôle de congestion est non sensible à la perte des paquets endommagés. Le taux de perte le plus élevée due à un paquet endommagé par fenêtre dégrade le débit du protocole TCP jusqu'à 60%.

9.2. Le délai périodique :

Les déconnexions fréquentes causent une condition appelée « Le délai périodique» à l'émetteur TCP. Ceci se produit au doublement de l'horloge de retransmission pour chaque tentative de retransmission infructueuse, pour réduire le taux de transmission. Puis, à la reconnexion du nœud mobile, TCP prendra beaucoup de temps pour récupérer une telle réduction et les données ne seront pas transmises pendant cette période de temps.

9.3. La variation de la taille du paquet :

Les liens sans fil supportent une taille des paquets généralement beaucoup plus petite par rapport à la taille des paquets dans des liens filaire. Donc, chaque paquet dans un réseau filaire est fragmenté lorsqu'il est transmis sous un lien sans fil. En conséquence, la récupération de la taille du paquet optimal dans des liens sans fil est une question clé pour les performances du réseau **[49].**

Le débit du TCP sans retransmission dans la couche MAC est inférieur à 23% que celui avec la retransmission dans la couche MAC. Les performances de l'UDP, même sans retransmission dans la couche MAC, sont un peu plus élevées que celles du TCP avec retransmission dans la couche MAC.

10. les services vidéo streaming adaptatifs:

D'après l'apparition de machines de plus en plus puissantes, l'Internet était utilisé pour partager et échanger des informations textuelles. Dans les années quatre-vingt, on commençait à l'utiliser aussi pour transmettre des contenus multimédia (séquence vidéo).

10.1 Définition :

Les services de streaming multimédia représentant une part de plus en plus importante du trafic web mondial, il devient primordial d'étudier les méthodes actuelles de diffusion afin de proposer des modèles plus intelligents permettant d'accompagner l'accroissement fort de son utilisation au niveau mondial. De plus, le transfert d'un multimédia d'un point d'origine à sa destination est critique sur la qualité perçue par l'utilisateur, car cela peut engendrer des perturbations importantes sur le service lui-même [57].

10.2 Le tampon (en anglais buffer):

Le tampon est un espace de stockage de données alloué qui contient des informations du flux que le visualiseur ou l'utilisateur est susceptible d'utiliser. Dans le cas d'un flux multimédia comme la musique ou un film, le tampon contient le contenu à venir que le spectateur n'a pas encore vu ou entendu. Le tampon peut également contenir du contenu affiché récemment pour un rembobinage rapide. Lors de la diffusion de programmes [56].

11. Conclusion :

Une description, faite dans ce chapitre, définitions général de réseau informatique, le modèle OSI et les différentes couches contenues et le fonctionnement du protocole TCP ainsi que ces mécanismes de contrôle de fiabilité (contrôle de flux, contrôle de congestion) et les algorithmes de Slow Start , Congestion Avoidance, AIMD, Fast retransmit et Fast-recovey.

Ce chapitre a présenté aussi quelques versions déjà proposées pour améliorer la performance de contrôle de congestion (TCP Taheo,TCP Reno,TCP New Reno…….) .

Etant donné que le sujet principal de ce mémoire est le contrôle de congestion dans le contexte de la mobilité, le chapitre suivant présentera, de façon un peu détaillée, quelques solutions proposées dans la littérature.

Chapitre 2

Etat de l'art

Chapitre 2 Etat de l'art

1. Approches proposées :

Dans le cadre de l'amélioration du protocole TCP dans le réseau sans fil en général et dans les réseaux ad hoc en particulier plusieurs approches ont été proposées. La plupart de ces approches visent a trouver une solution qui permet au protocole TCP de faire la différence entre les pertes de paquets due a la congestion du lien et les pertes de paquets qui sont due aux erreurs des lien.

2. Différentes versions d'amélioration du protocole TCP dans les réseaux sans fil:

2.1. Ad hoc TCP (ATCP):

ATCP **[50],** TCP ad hoc utilise lui aussi une réponse de retour de la couche réseau. En plus des échecs de route, ATCP a pour but de régler le problème des taux d'erreur élevés de bits (BER).

Le TCP émetteur peut se mettre dans l'un des états suivant :

-Etat persistant : perte de paquets due à un échec de route

-Etat de contrôle de congestion : perte de paquets due à une vraie congestion de réseau.

-Etat de retransmission : perte de paquets due à un taux d'erreur de bit élevé.

Une couche appelée ATCP est insérée entre la couche TCP et IP du nœud source. ATCP lit l'information de l'état du réseau donnée par le message 'ECN' (explicit congestion Notification) et le message 'ICMP' (Destination inaccessible) et par la suite, l'ATCP met l'agent TCP dans l'état approprie selon la réponse reçue.

. A la réception d'un message 'ICMP', l'agent TCP entre dans un état persistant, durant lequel

L'agent est gelé et aucun paquet n'est transmis jusqu'à qu'une nouvelle route est retrouvée par l'exploration du réseau, et donc l'émetteur ne peut pas invoquer un contrôle de congestion

A la réception d'un message 'ECN', invoque un contrôle de congestion sans attendre l'événement de Time Out pour détecter les pertes de paquets dues à une erreur de transmission.

ATCP contrôle les acquittements reçus, quand ATCP remarque qu'il a reçu trois (03) acquittements dupliqués, il mit le TCP dans état persistant et retransmis rapidement le paquet perdu à partir du buffer.

Après la réception d'un acquittement non dupliqué, ATCP mis TCP dans un état normal.

Comme avantages de la solution A-TCP **[50]** on trouve :
Permettent à la solution A-TCP de fonctionner sur Internet.
Elle fournit une solution Possible et efficace pour améliorer le débit du TCP dans les réseaux sans fil ad hoc.
Parmi les inconvénients de cette solution on cite :
La dépendance du protocole de la couche réseau pour détecter les changements et les partitions ne peut pas être implémentée par tous les protocoles de routage, l'ajout de la couche ATCP dans la pile protocolaire du modèle TCP/IP nécessite des changements dans les interfaces actuellement utilisées.

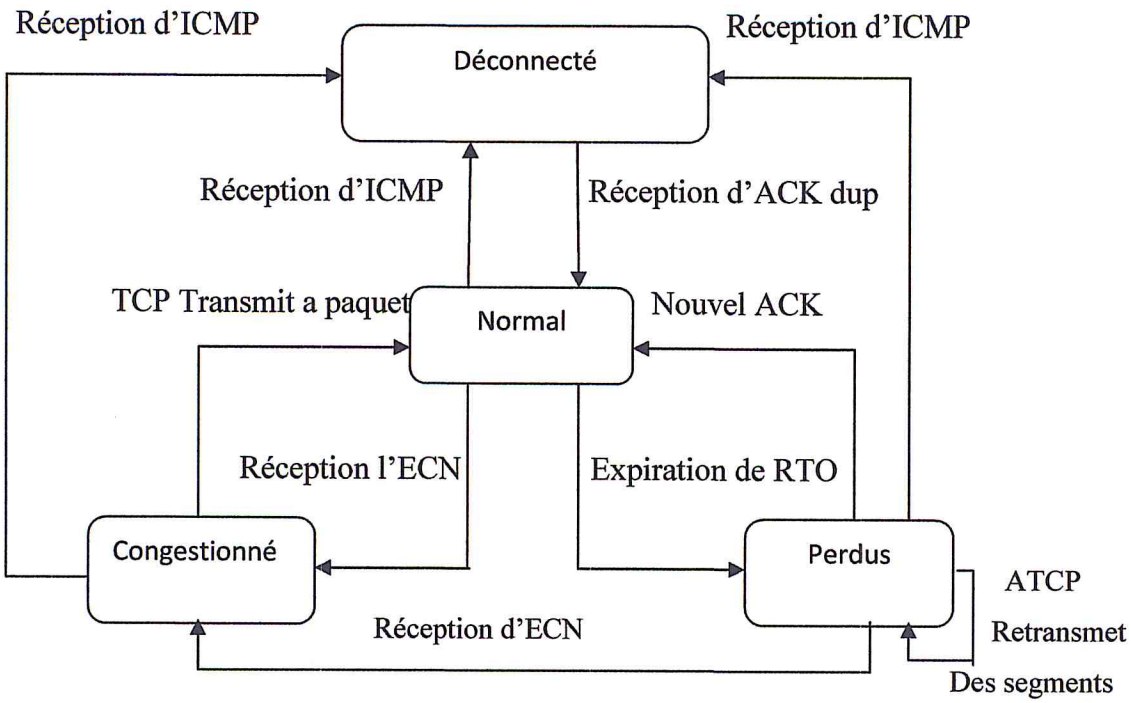

Figure16: Diagramme état de transition ATCP(Emetteur).

2.2. Detection of Out Of Order and Response (TCP-DOOR) [51]**:**

Cette approche est la solution de bout en bout qui ne nécessite pas la coopération de nœuds intermédiaires, elle est basée sur des événements Out-Of-Order (OOO). Les événements (OOO) sont interprétés comme une indication d'échec de route. La détection des **O.O.O** est accomplie soit par un mécanisme basée sur expéditeur ou bien d'un mécanisme basé sur le récepteur à travers des informations qui est insérée aux paquets des acquittements, et les segments de données.

De côté émetteur, cette technique se base sur la propriété de numéro de séquence des acquittements 'Sequence Number'. Dans le cas, des paquets d'acquittements dupliqués qui auront le même numéro de séquence et par conséquent pour détecter l'**O.O.O**, l'émetteur a besoin d'une information supplémentaire, celle-ci est un octet optionnel ajouté à l'ACK, appelé "ACK Duplication Séquence Number" (**ADSN**), qui sera incrémenté et transmis avec chaque ACK dupliqué.

Cependant, le récepteur a besoin de deux (02) octets optionnels pour détecter les **O.O.O**, appelé "TCP Packet Séquence Number" (**TPSN**), qui est incrémenté et transmis avec chaque segment de données incluant les paquets retransmis.

Si le récepteur détecte un événement **O.O.O**, il doit informer l'émetteur par la mise à jour d'un bit optionnel dans l'entête du paquet d'Ack, appelé "**O.O.O bit**". Une fois l'émetteur, s'informe sur l'événement, il doit prendre l'une des actions suivantes pour réagir. La première action, le TCP émetteur garde des variables d'état tel que le RTO et la taille de sa fenêtre Cwnd constantes durant une période de temps T1. La deuxième action, si durant une période temps passé T2, l'émetteur est entré dans la phase de l'évitement de congestion, il devrait récupérer immédiatement l'état avant l'invocation de contrôle de congestion.

Comme avantages de la solution TCP DOOR **[51]** on trouve :
- le protocole TCP-DOOR améliore le rendement de 50%
- l'approche peut travailler sur tout type d'environnement et d'offrir encore une amélioration significative

Parmi les inconvénients de cette solution on cite :
-Les protocoles de routage multi-route peuvent produire des événements OOO qui ne sont pas liés à des défaillances de route.

2.3. Sélection Path à base de retenue (COPAS):

Dans **[52]**, les auteurs abordent le problème de baisse de la performance de TCP en raison des concurrences d'accès sur un canal sans fil. Un nouvel algorithme est proposé, appelé COPAS, qui intègre deux mécanismes pour améliorer les performances TCP en évitant les conditions de capture.

Tout d'abord, il utilise les chemins disjoints vers l'avant (émetteur vers le récepteur pour les données TCP) et vers l'arrière (récepteur vers l'expéditeur pour TCP ACK) afin de minimiser les conflits de données TCP et les paquets ACK.

Deuxièmement, COPAS emploie un schéma d'équilibrage de contenance dynamique où il surveille et change continuellement les chemins disjoints avant et arrière en fonction du niveau de contention de la couche MAC, minimisant ainsi la probabilité de capture.

Une fois la contention d'une itération dépasse un certain seuil, appelé seuil de temporisation, une nouvelle itération moins contentieuse est choisie pour remplacer la route contentieuse.

Comme avantages de la solution TCP COPAS **[52]** on trouve :

- Grâce à une simulation étendue, COPAS permet d'améliorer le débit TCP jusqu'à 90% tout en réduisant les frais généraux de routage

- . COPAS peut être déployé de tout protocole de routage à la demande, tel que DSR et AODV.

2.4. TCP puissance de signal :

Dans **[53]**, les auteurs proposent des mécanismes qui sont basés sur des mesures de résistance du signal pour atténuer les pertes de paquets en raison de la mobilité. Les idées clés sont :

A-Si les mesures de la force du signal indiquent qu'une défaillance de la liaison est vraisemblablement due à un voisin qui se déplace hors de portée, en réaction, facilite l'utilisation d'une puissance d'émission temporaire plus élevée pour maintenir le lien en vie

B-Si les mesures de résistance du signal indiquent qu'un lien risque d'échouer, lancez une nouvelle découverte de l'itinéraire de manière proactive avant que le lien échoue réellement.

Dans cette algorithme ,chaque nœud conserve se sauvegarder la puissance de signal reçu de nœud adjacents , à partir de ces enregistrement le protocole de routage prédit immédiatement les échecs de route ,cette prédiction appelle (proactive Link management) .Apres chaque saut vers un nouveau nœud de la route ,si détecter un route un échec de route ,l'agent de routage de la source est averti par le message ' going down' ,durant à la réception de ce message l'agent de routage de la source arrête d'envoyer des paquets et activer une procédure de recherche une nouvelle route à partir de mécanisme appelé (réactif du link management), ce mécanisme augmente la puissance de transmission pour rechercher des nouvelle routes à chaque fois qu'une erreur de route.

Les mécanismes de gestion de liens proactifs et réactifs permettre de prédire les pannes de lien, l'agent de routage du nœud informe la source pour arrête l'envoi de paquets, ce nœud augmente sa puissance d'émission pour bien gérer les paquets en transit qui utilise si lien.

Comme avantages de la solution TCP avec puissance du signal **[53]** on trouve :

-Cette approche donne 45% d'amélioration sur les performances du protocole TCP.

Parmi les inconvénients de cette solution on cite :

- La simulation utilisée dans les réseaux faiblement chargés.

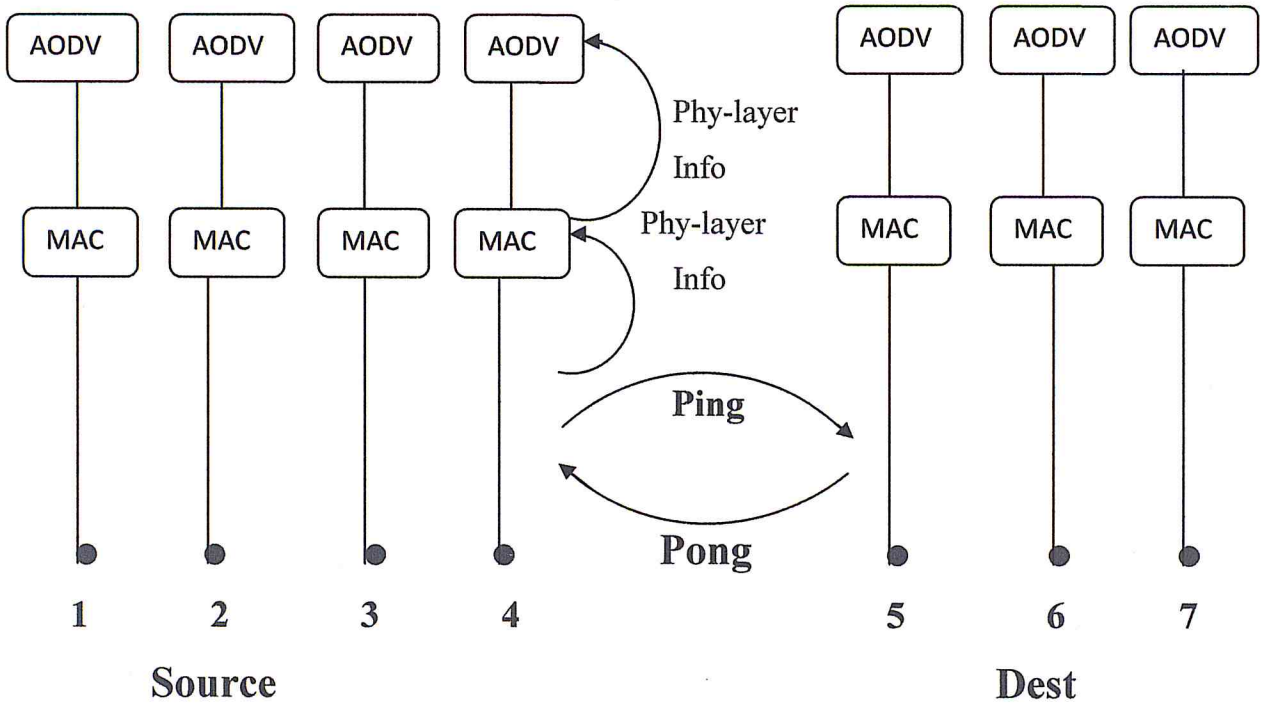

Figure 17: Inter-couches réseau et physique

2.5. HYBRID TCP:

Dans **[54]**, généralement, le TCP n'est pas vraiment compatible avec les réseaux sans fil, car TCP considère que toutes les pertes de paquets sont dues à la congestion, ce fait dégrade les performances du réseau. Par conséquent, pour résoudre ce problème de compatibilité, plusieurs approches ont été proposées .La plupart de ces approches utilisent une solution de couche croisée qui échappe à la notion pure de cascade du modèle de communication OSI avec des limites pratiquement strictes entre les couches. L'approche de couche croisée transmet les retournements dynamiquement via les limites de la couche pour permettre la compensation en tant que méthode. Le but de ce travail est de fournir une solution de couche croisée basée sur la formule RTT de V. Jacobson et exploite la puissance du signal sans fil et la valeur du bruit pour améliorer TCP dans les MANET. La particularité de l'approche est qu'elle prend en compte l'environnement externe du réseau.

Dans la solution proposée dans **[54]**, la puissance du signal et la valeur du bruit de l'environnement sans fil sont considérées comme des facteurs pour déterminer comment réagir à la perte de paquets. Ils sont utilisées pour calculer la valeur estimée du temps aller-

retour dans le cas normal (RTT estimé) et le compare avec le RTT réel pour déterminer la cause de la perte et agir selon l'analyse.

Afin de détecter la cause réelle de la perte de paquets lorsqu'elles se produisent dans un environnement sans fil mobile et régir ensuite, dans [55], les auteurs ont intégré dans la structure TCP deux nouvelles variables, la première variable s'appelle LSS (la valeur minimale de puissance de signal) qui contient la valeur la plus basse de la puissance du signal de tous les sauts entre l'émetteur et le récepteur, la deuxième variable s'appelle HNV (valeur maximale de bruit), représente la plus grande valeur de bruit de l'environnement sans fil. Pour intégrer ces variables (LSS, HNV), les auteurs ont utilisé une solution de couche croisée, la valeur de puissance du signal et la valeur du bruit sont des variables de couche physique, il n'est pas possible de les intégrer dans la couche de transport sans utiliser cette méthode.

Ces deux variables sont utilisées pour détecter la cause réelle de la perte de paquets. Lors de la transmission de données, la perte entre l'expéditeur et le récepteur sur une zone sans fil utilisant TCP avec une connexion multi-sauts, chaque nœud reçoit le paquet avant de transférer au prochain nœud, il met à jour la valeur de LSS et HNV

- Si la valeur de la puissance du signal du nœud actuel est inférieure à LSS, LSS prend comme valeur la valeur du nœud actuel de la puissance du signal, sinon elle ne fera rien.
- Si la valeur de bruit du nœud actuel est supérieure à HNV, alors HNV prend comme valeur la valeur actuelle du bruit du nœud, sinon il ne fera rien.

Après avoir mis à jour ces deux valeurs, il envoie le paquet au nœud suivant jusqu'à ce que le paquet arrive à sa destination.

Pour décider qu'une perte de paquet s'est produite, après l'envoi d'un paquet, l'expéditeur attend une valeur RTT du temps; Si il ne reçoit pas un paquet ACK (accusé de réception) du récepteur, il décide que le paquet envoyé a été perdu.

Pour estimer combien du temps l'expéditeur doit attendre avant d'être sûr que le paquet envoyé a été perdu, TCP utilise une formule, cette formule fonctionne bien avec les réseaux câblés, mais pas avec le MANET. Pour adapter cette formule aux MANETS, nous avons introduit de nouveaux facteurs qui sont la force du signal et le bruit, plus la valeur de la puissance du signal est plus faible et la valeur du bruit est plus importante, plus le temps d'attente sera plus grand.

3. Comparaison général et discutions :

Plusieurs solutions qui ont été proposé pour améliorer la performance TCP dans le réseau sans fil mobile comme (ATCP, TCP DOOR, COPAS, TCP avec puissance du signal, TCP hybrid) Chaque solution a des avantages et des inconvenants.

Le tableau suivant récapitule les approches vues en mentionnant une comparaison entre ces approches :

Proposition	Type de solution	Degré de complexité	Type de réseau	Nombre de connexion	Débit	Évaluation
ATCP [50]	Inter-couches	haute	Mobile aléatoire	Mono saut	Haut	Emulation
TCP-DOOR [51]	Couche TCP	faible	Mobile aléatoire	Mono saut	moyenne	simulation
Signal strength Based link [53]	Inter-couches	haute	Mobile aléatoire	Deux sauts	Faible	simulation
COPAS [52]	Couche réseau	Moyen	Statique aléatoire	Multi-sauts	Haut	Simulation
HYBRID TCP [54]	Inter-couches	Haute	Mobile aléatoire	Multi-sauts	Haut	Simulation

Tableau 2 : comparaison entre les versions de performance TCP

4. Conclusion :

D'après l'étude et l'analyse les différents approches qui essaient d'améliorer le comportement et les performances du protocole TCP dans les réseaux sans fil, nous avons constaté qu'il y'a plusieurs façons et techniques qui peuvent être utilisées et qui donnent de bons résultats et de bonnes performances. Parmi ces solution, l'approche hybrid TCP c'est la meilleure solution qui donne plusieurs avantages (haut débit, haute degré de complexité, type de réseau : mobile aléatoire, nombre de connexion : multi-saut).pour cela, nous avons décidé de travailler avec cette solution. L'approche a été validés par une simulation, les résultats ont démonté l'efficacité et montré une bonne performance. Un des inconvenants de cette solution c'est que développer dans la simulation, afin de améliorer cette solution, nous avons choisi de développer cette solution dans le cas réel d'émulation

Problématique et objectif :

La pile protocolaire TCP/IP du modèle en couches a assuré pendant une période assez longue un transport de données de bout en bout efficace et fiable. Au cours des ans, des versions successives de TCP ont vu le jour, dans le but d'optimiser les performances du protocole TCP.

Néanmoins, ces améliorations ont été réalisées dans le contexte des réseaux filaires.L'avènement des réseaux sans fil, en particulier les réseaux mobiles, a mis au jour des comportements indésirables de TCP,à cause du faite que dans tels type de réseaux, les terminaux portables peuvent se déplacer fréquemment tout en communiquant. Pendant ces mouvements, les données transmises ou à recevoir par l'hôte mobile peuvent être perdues pour plusieurs raisons (interférences, congestion, mobilité…)

Le protocole TCP interprète ces pertes comme une situation de congestion du réseau même si la perte n'est pas due à la congestion (interférences, mobilité…) et active les mécanismes appropriés (contrôle de congestion, contrôle de flux, retransmission,…), ce qui dégrade fortement les performances du réseau. Dans le contexte de la gestion des pertes de paquets du aux facteurs du réseau sans fil, plusieurs contributions ont été récemment proposées, elles visent à adapter le protocole TCP aux réseaux mobiles.

L'un des plus grand inconvenants de la solution [54] et ce malgré les bons résultats obtenu est l'apport du concept inter-couches ou cross-layer dans la solution proposée qui la rend difficile à implémenter dans une émulation, Quelque chose qui n'ont pas réalisable dans l'émulation car le modèle OSI marche dans une seul sens. Comme objectif principale dans ce mémoire, on va tenter de proposé une modification à l'approche [54] afin de la rendre favorable à une implémentation dans un cas réel d'émulation. En essayant de prédire les valeurs de puissance de signal de la communication en cours à partir des communications précédents sans descendre à la couche physique pour déterminer le vraie cause de la perte de paquets sur le réseau(congestion ,mobilité….) afin d'améliorer les performances de TCP dans les réseaux sans fil selon le type de perte.

Chapitre 3

Conception

Chapitre 3 La conception

1. Introduction :

Le but de ce chapitre est de trouver une solution qui vise à améliorer les performances de TCP dans le réseau sans fil. La simulation de la solution TCP hybride montre les performances de cette dernière. Mais, afin de compléter l'évaluation de cette dernière on propose méthode d'implémentation de cette dernière dans un environnement réel (émulation de la solution), Contrairement à la simulation, l'émulation d'une solution nécessite des véritables machine qui exercent des communications dans un environnement réel. L'objectif est basé sur la puissance du signal reçu qui sert à déterminera le vraie cause de la perte de paquets sur le réseau afin d'améliorer les performances de TCP dans les réseaux sans fil.

2. Récupération de la valeur du RSSI:

La valeur de la puissance du signal reçu est récupérée par le récepteur à partir de la couche physique à chaque réception de paquet. Cette valeur est mesurée en 'dbm' qui est le rapport de puissance entre la puissance mesurée en décibel (db) et un milliwatt (mW).

3. Estimation de la puissance de signal du prochain paquet à recevoir:

3.1 Formulation de la solution proposée :

Afin d'adapter le mécanisme de perte de paquet et de contrôler le mécanisme de congestion de TCP dans le réseau sans fil, on a commencé par prédire la prochaine valeur de puissance du signal en se basant sur les cinq derniers valeurs de puissance du signal. D'abord on récupère les cinq valeurs de puissance de signal avec un intervalle de 3 secondes entre valeur et valeur. On a choisi de considérer un intervalle de trois seconds vu qu'avec une vitesse de déplacement moyenne d'un humain (du nœud), cet intervalle est suffisant pour impacter la puissance du signal.

Ensuite, nous étudions les changements de puissance du signal en utilisant les relations suivantes :

$V1 = S4 - S3$ .....(1)

$V2 = S3 - S2$ .....(2)

$V1 = S2 - S1$ .....(2)

Après nous calculons la moyenne de la variation de la puissance du signal afin de prédire la prochaine puissance du signal:

$RES = (V1+V2+V3)/3$ .....(4)

Enfin, à l'aide de la formule (5) on prédit la valeur de la prochaine puissance du signal.

$PSE = S5 + RES$ .....(5)

Suite à l'estimation de la prochaine valeur de RSSI. En cas de perte de paquets, TCP utilisera cette valeur on la comparant à un seuil de puissance de signal pour tronchet sur la raison de perte de paquet (congestion ou mobilité) afin d'améliorer les performances du réseau.

La valeur du seuil de puissance de signal de la carte réseau est donnée par son constructeur.

Si la valeur de puissance du signal estimée est supérieure à la valeur du seuil de la carte réseau, TCP déduira que la perte est due à la mobilité, dans ce cas notre mécanisme désactive la fenêtre de flux de TCP temporairement (TCP window scaling = 0) pour permettre de garder un débit élevée.

Sinon, si la valeur de puissance du signal estimé est inférieur ou égale à la valeur du seuil de puissance du signal, TCP déduira que la perte de paquets a été provoqué par une congestion du réseau, donc notre mécanisme réactivera le mécanisme de réduction de la fenêtre de flux de TCP (TCP window scaling = 1)

3.2 Algorithme descriptif du mécanisme proposé:

Début

Pour i=1 à 5

faire

PSMRi = get(Si) ; // récupérer la puissance du signal

Ajouter chaque valeur au tableau (T[i] = PSMRi)

If (i<5) alors

Déclencher timer(3secondes)

Fsi

Fait ;

Tantque (2<3) //boucle infinie

Faire

V1 = T[4] - T[3], V2 = T[3] - T[2], V3= T[2] - T[1] ; // chaque fois comparer les changements de puissance du signal

MCPS = (V1+V2+V3)/3 // MCPS c'est la moyenne de changement de la puissance du signal dans les 4 premier valeurs

PSE = t [5] + MCPS ; // la valeur de l'estimation

Seuil = get(seuil); // récupération de la valeur de seuil signal de la carte réseau

If (PSE>Seuil) alors

Exécute (désactiver le mécanisme de réduction de fenêtre TCP) ; // car la possibilité de congestion est faible

Sinon

Exécute (activer le mécanisme de réduction de fenêtre TCP) ; // pour soulage la congestion ;

Fsi ;

T [1] = T [2],

T [2] = T [3],

T [3] = T [4],

T [4] = T [5];

Déclencher timer (3 secondes) ;

PSMR5= get(S5) ; // S5 la puissance du signal après 3 secondes ;

Ajouter chaque valeur au tableau (T [5] = PSMR5)

Fait ;

Fin

4. Organigramme de la solution proposée :

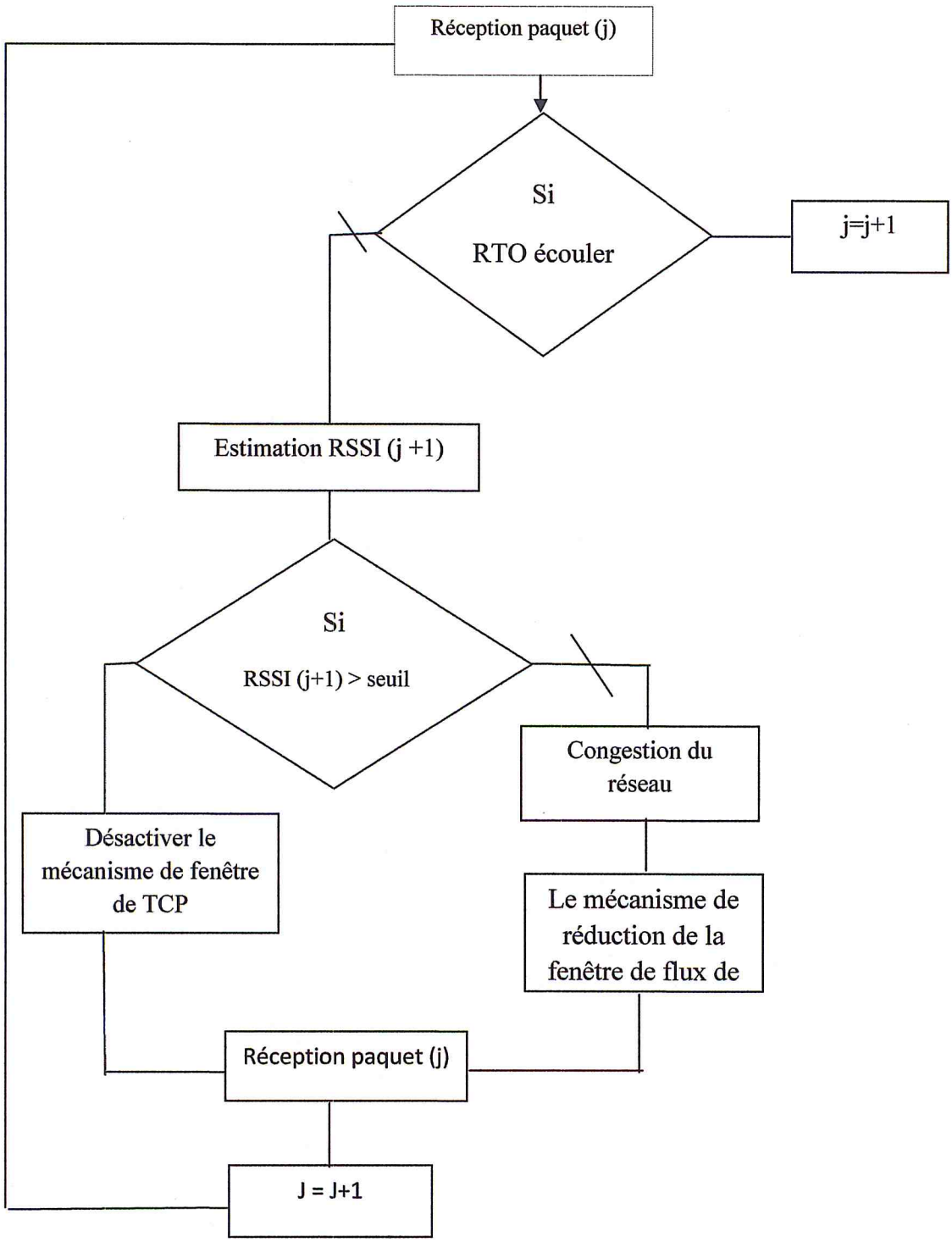

Figure 18 : Organigramme de la solution proposée.

5. Conclusion :

Dans ce chapitre nous avons proposé un mécanisme qui vise à estimer la puissance du signal du prochain paquet au lieu de la récupérer directement en utilisant la simulation. En se basant de récupérer les valeurs de puissance de signal des communications précédents pour prédire les valeurs de puissance de signal de la communication en cours. En cas de perte de paquets, cette valeur vu aider le mécanisme de perte de paquets de TCP à faire la distinction entre les pertes dues à la congestion et ceux dues à l'environnement sans fil (mobilité), afin d'améliorer les performances de TCP dans les réseaux sans fil.

Chapitre 4

Implémentation et évaluation

Chapitre 4 l'implémentation et l'évaluation

1. Introduction :

Dans ce chapitre, nous présentons l'environnement d'émulation et de développement choisis, l'amélioration des services streaming adaptatifs d'après étudie les variations de la puissance du signal et les changements de charge de la mémoire tampon 'buffer health' au cours du temps, les différents schémas de l'implémentation de notre système et nous discutons les résultats de l'émulation.

2. Environnement de l'implémentation :

L'implémentation et la validation de notre approche a été réaliser dans un environnement linux (Ubuntu). Celui-ci est un système d'exploitation GNU/Linux basé sur la distribution Linux Debian, Ubuntu se définit comme un système d'exploitation utilisé par des millions de PC à travers le monde, avec une interface « simple, intuitive, et sécurisée ». Il est la distribution la plus consultée sur Internet d'après le site Alexa [55]

.Durant l'émulation, deux scénarios ont été considérés. Le but était de comparer l'approche que nous avons proposée avec une autre version de TCP, qui est le TCP de Ubuntu (TCP Reno) afin de vérifier la performance de notre approche.

Notre modèle d'émulation est basé essentiellement sur les principes suivants:

-Une topologie de réseau ad hoc composée de 2 nœuds
- Chaque nœud est mobile et décide seul de ses déplacements
- Le transfert de paquets se fait en mono-saut.

- Le débit de transfert maximal est de 50 Mbps.
- Les données utilisées sont des données multimédia (séquences vidéo).
- Les nœuds ne sont pas sous l'effet des interférences.

3. La méthode d'étude de puissance du signal varie avec le temps :

La puissance du signal reçu ou le RSSI joue un rôle très important dans la bonne transmission des paquets dans les réseaux sans fil. Nous étudions la variation de la puissance du signal au cours du temps suivant les étapes suivant :

- Lancer une vidéo multimédia avec une qualité du vidéo 480 pixel.
- Dans chaque dix secondes récupéré la valeur de la puissance signal jusqu'à l'obtention de six valeurs de puissance du signal dans le même endroit.
- A chaque fois augmenté la distance d'un mètre et demi et refaire la même étape précédente.

Sachant que la valeur de puissance du signal est négative, plus la valeur absolu de la puissance du signal en dbm est proche de 0 plus cela signifie que la puissance du signal est bonne. Contrairement, Plus la valeur absolu de puissance de signal est grande plus cela signifie que la puissance du signal est mauvaise. Pour faciliter la vision, nous ajouterons 100 à chaque puissance de signal pour obtenir des valeurs positives, dans ce cas, plus la valeur de puissance du signal est élevée, plus la puissance est fort, le contraire est vraie.

3.1. Résultat obtenus et discutions:

Les résultats de chaque distance sont représentés par des graphes suivants :

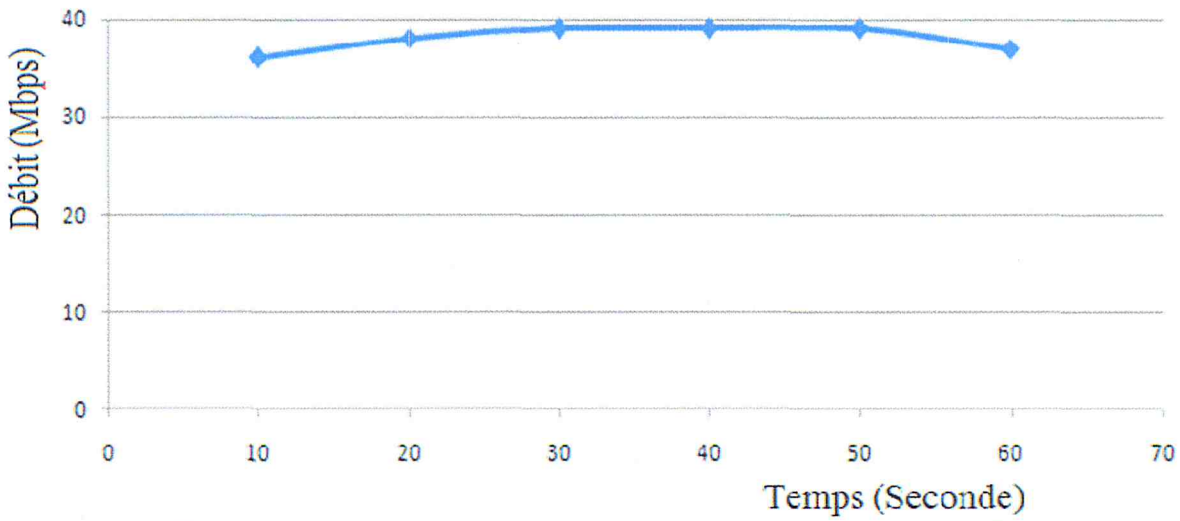

Figure 19 : le résultat de la puissance signal dans la distance 9.5 m

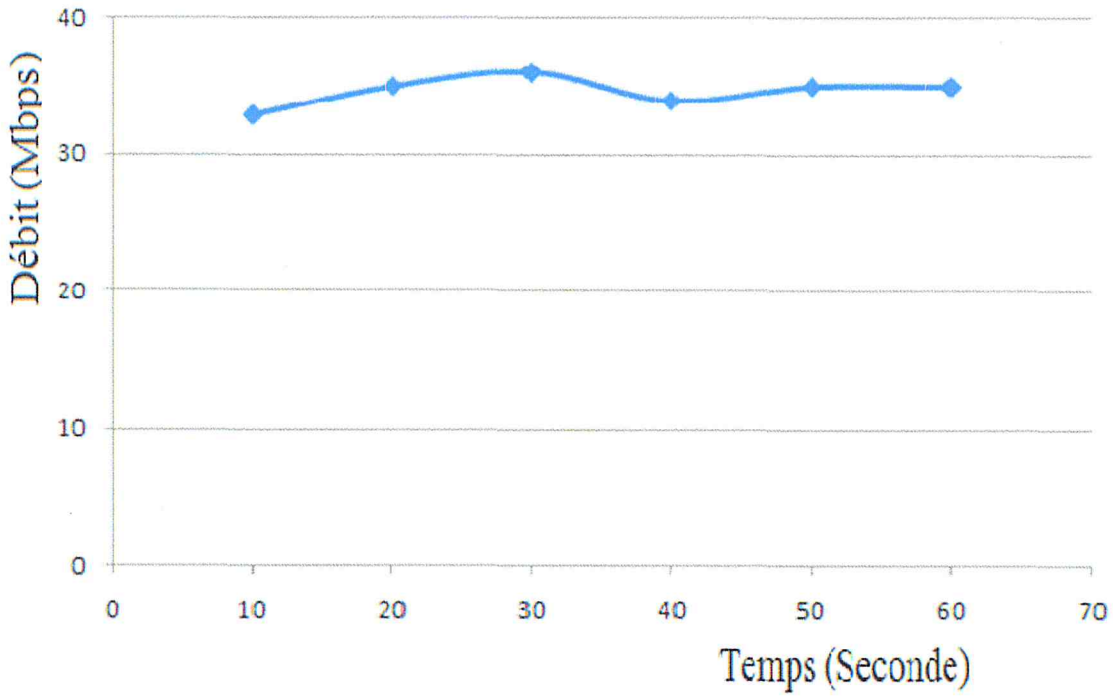

Figure 20: le résultat de la puissance signal dans la distance 11 m

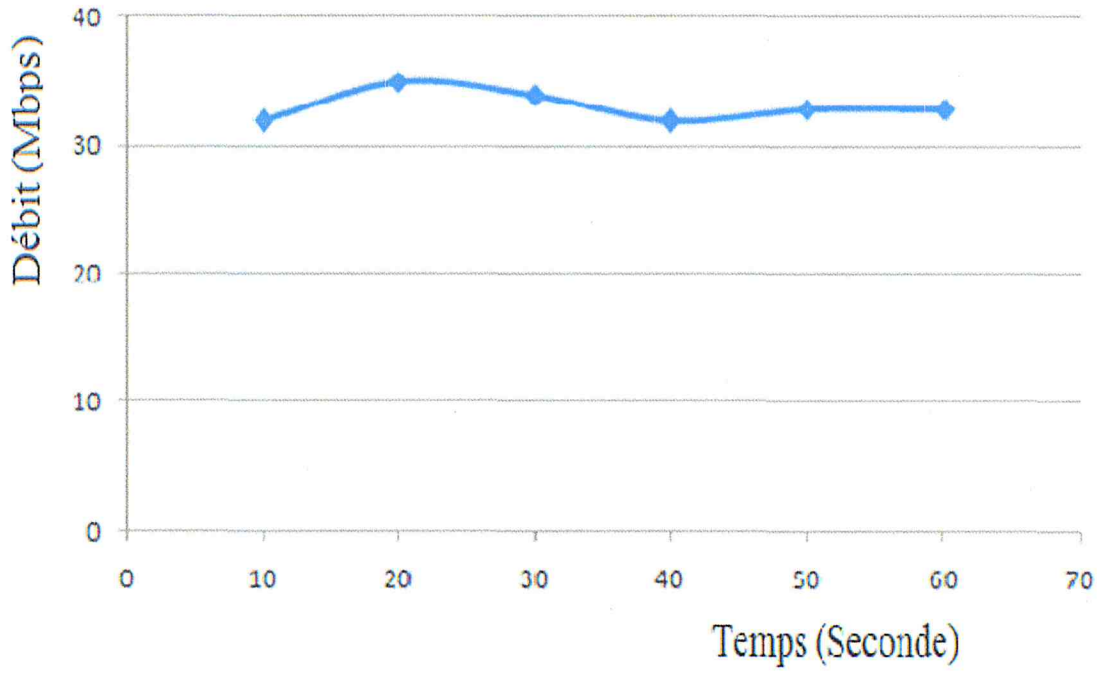

Figure 21: le résultat de la puissance signal dans la distance 12.5 m

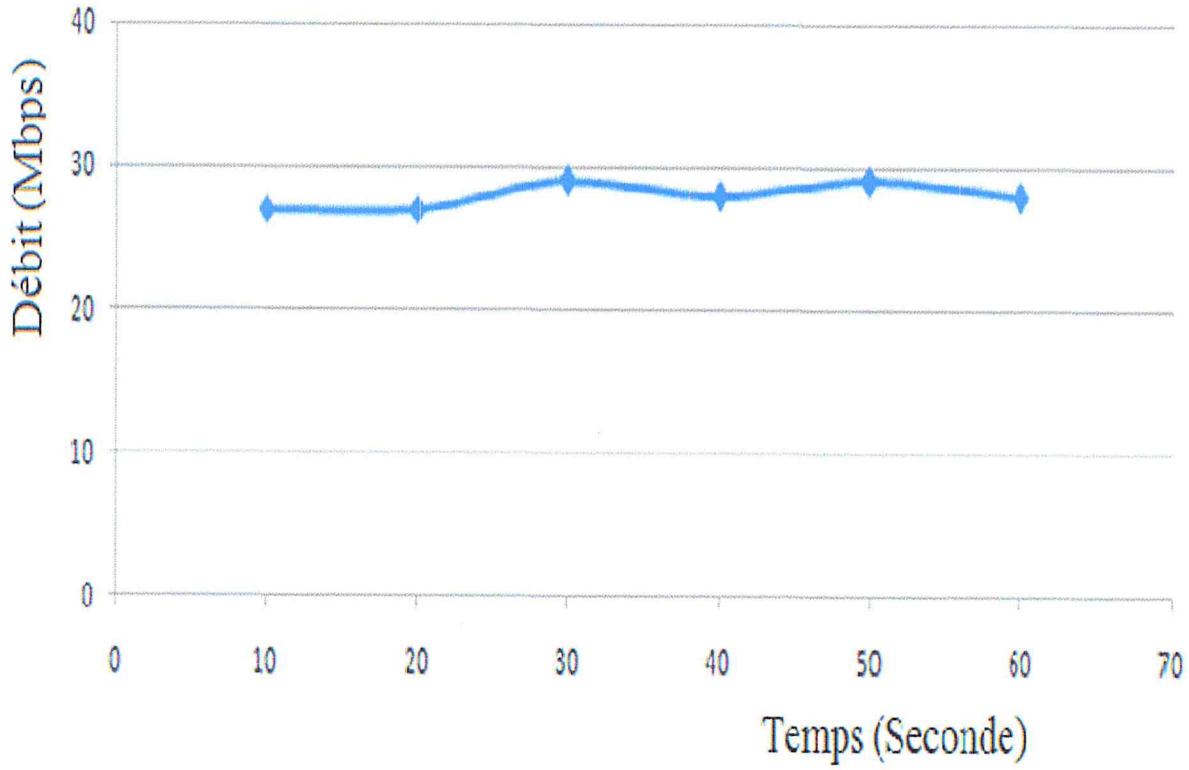

Figure 22 : le résultat de la puissance signal dans la distance 14 m

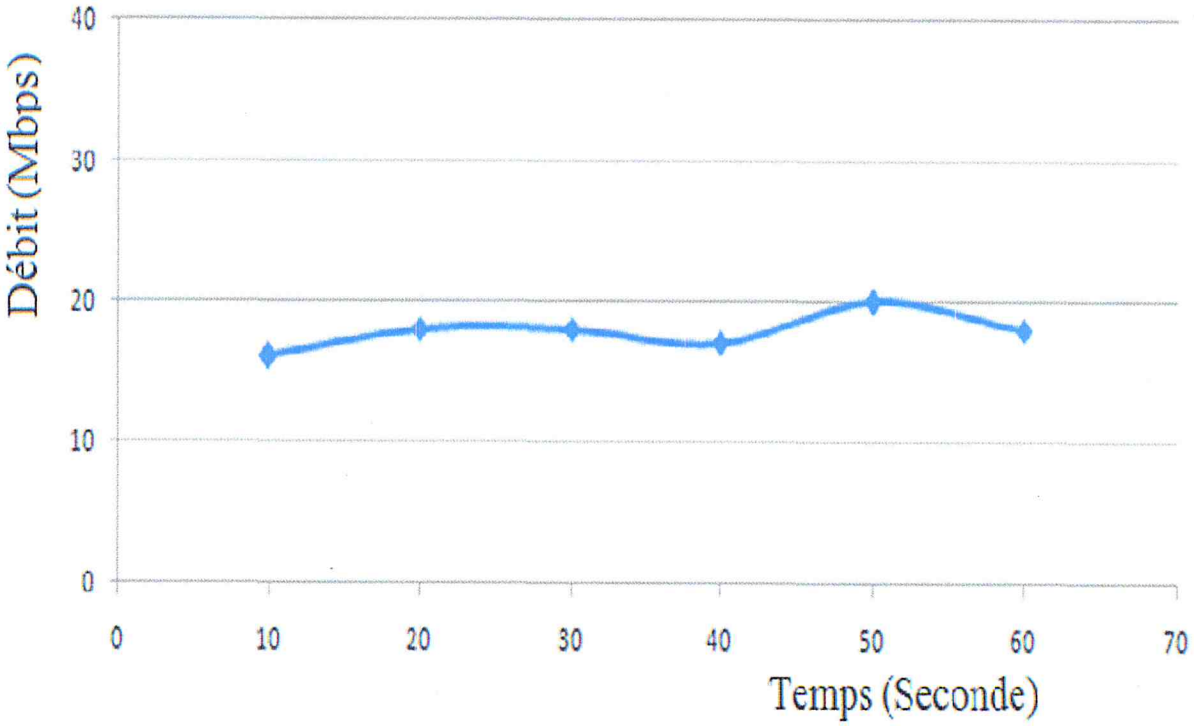

Figure 23 : le résultat de la puissance signal dans la distance 15.5 m

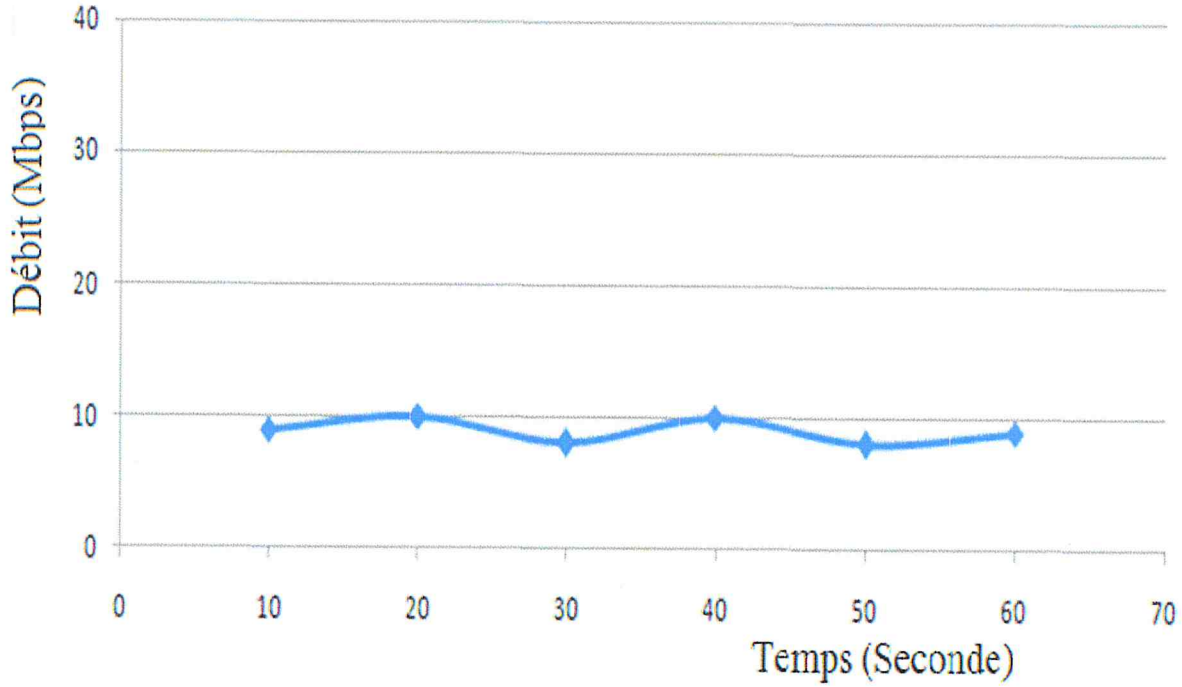

Figure 24 : le résultat de la puissance signal dans la distance 17 m

3.2. Interprétation :

A travers les graphiques, on constate que plus distance est grande, plus la puissance de signal reçu est faible et donc le nœud sans fil est loin de la zone de couverture sans fil. Sa puissance de signal reçu diminue (le nœud) jusqu'à ce qu'elle atteint un certain seuil ou la transmission s'arrête complètement.

Contrairement, plus la distance est petite, plus la puissance de signal reçu est meilleure.

Enfin, les valeurs de signal récupéré au même endroit sont presque identiques.

3.3 Seuil de puissance de signal :

Normalement chaque carte réseau a un seuil minimal de puissance du signal donné par son constructeur, mais comme les cartes réseau que nous possédons ne sont pas récentes et professionnelles, on n'a pas cette information.

Afin de déterminer cette valeur de seuil on s'est basé sur les résultats des tests qui ont été faites précédemment de la variation de la puissance du signal ainsi que ceux de la figure 30.Nous avons déduit que la puissance du signal atteint le seuil de la carte réseau à la distance de 14 mètres qui est équivalent à une puissance du signal qui est égale à 30 dpms (-70 dpms dans la

valeur réel). A partir de cette valeur de seuil la communication commence à ce dégradé à cause des pertes provoquées par la distance entre les deux nœuds.

4. L'émulation de la solution:

Pour tester le comportement de notre approche. On va étudie la variation de la vitesse de remplissage du buffer health du service de vidéo streaming (YOUTUBE) au cours du temps. Cela a été fait suivant les étapes suivantes :

- Lancer une vidéo multimédia (YOUTUBE) avec une qualité vidéo de 480p.

- Chaque dix secondes on récupère la valeur du buffer health dans une distance précise jusqu'à la fin de vidéo (durée du vidéo 2min et 34 s).

-Nous avons répéter l'étape précédente plusieurs fois avec plusieurs distances (à chaque fois on s'éloigne d'un mètre et demi).

- Faire toutes les étapes précédentes avec les deux versions de TCP étudié.

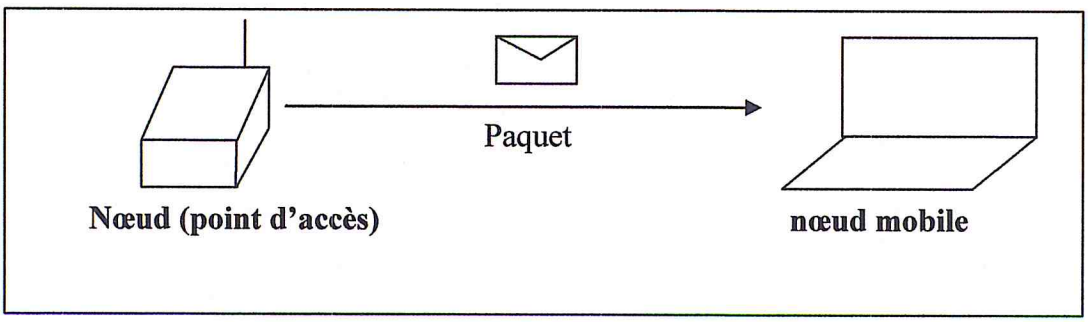

Figure 25 : Topologie de la simulation

4.1. Résultat obtenus et discutions:

Les résultats de chaque distance sont représentés par des graphes suivants :

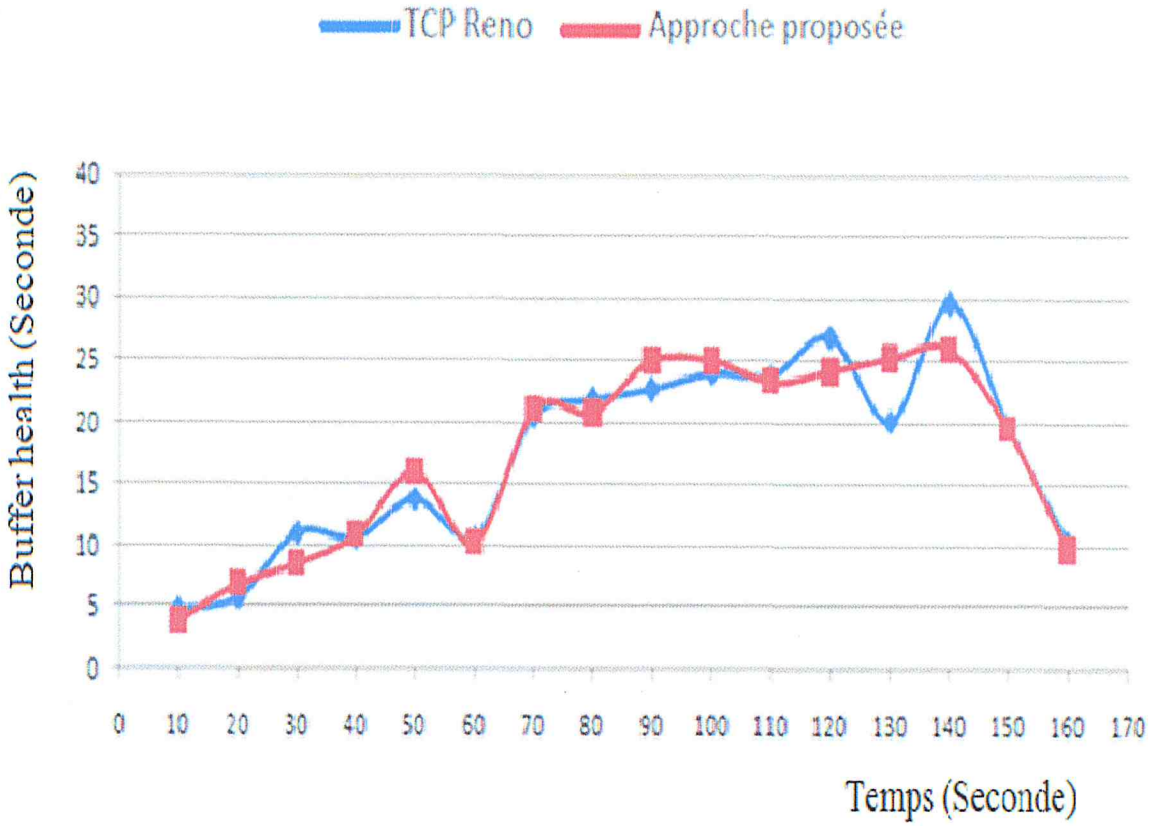

Figure 26 : le résultat du buffer health dans la distance de 9.5 m

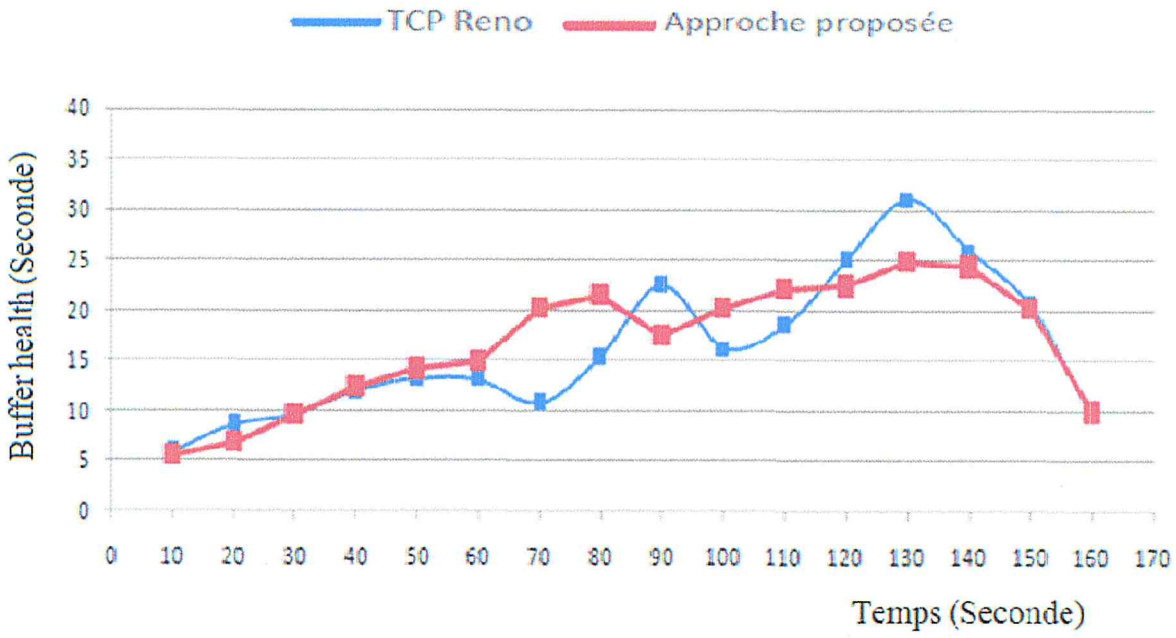

Figure 27 : le résultat du buffer health dans la distance 11 m

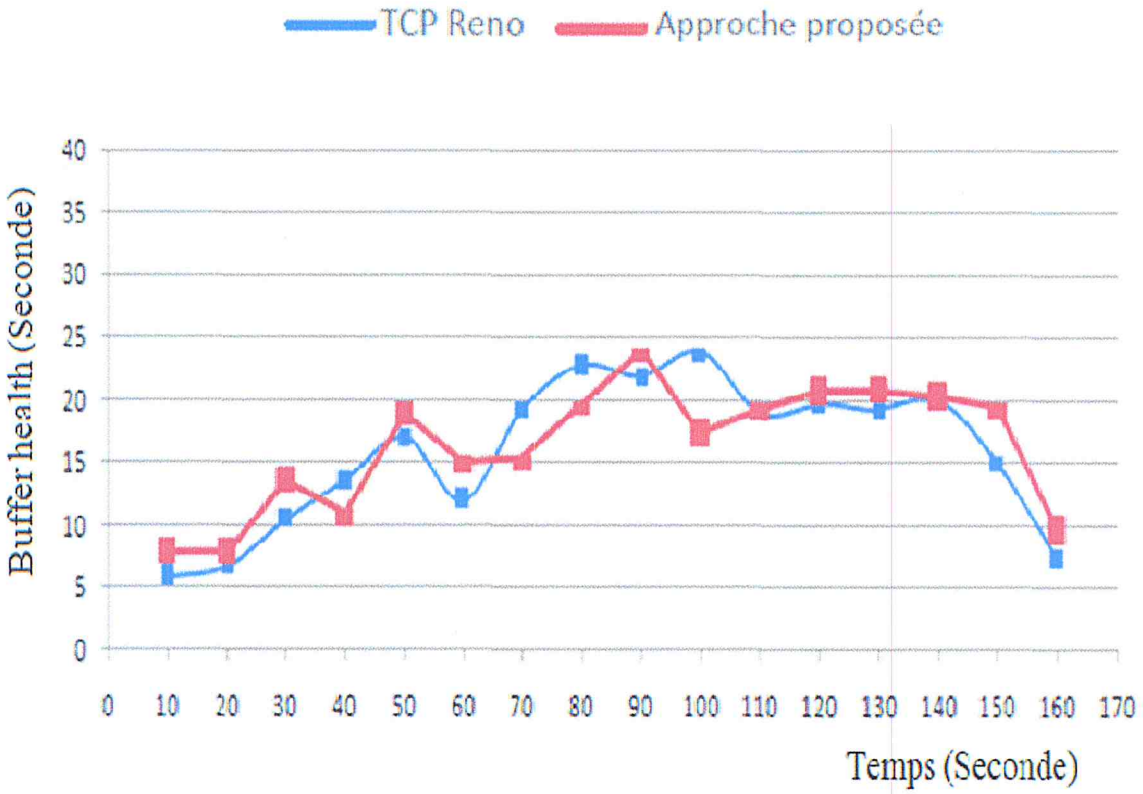

Figure 28 : le résultat du buffer health dans la distance 12.5 m

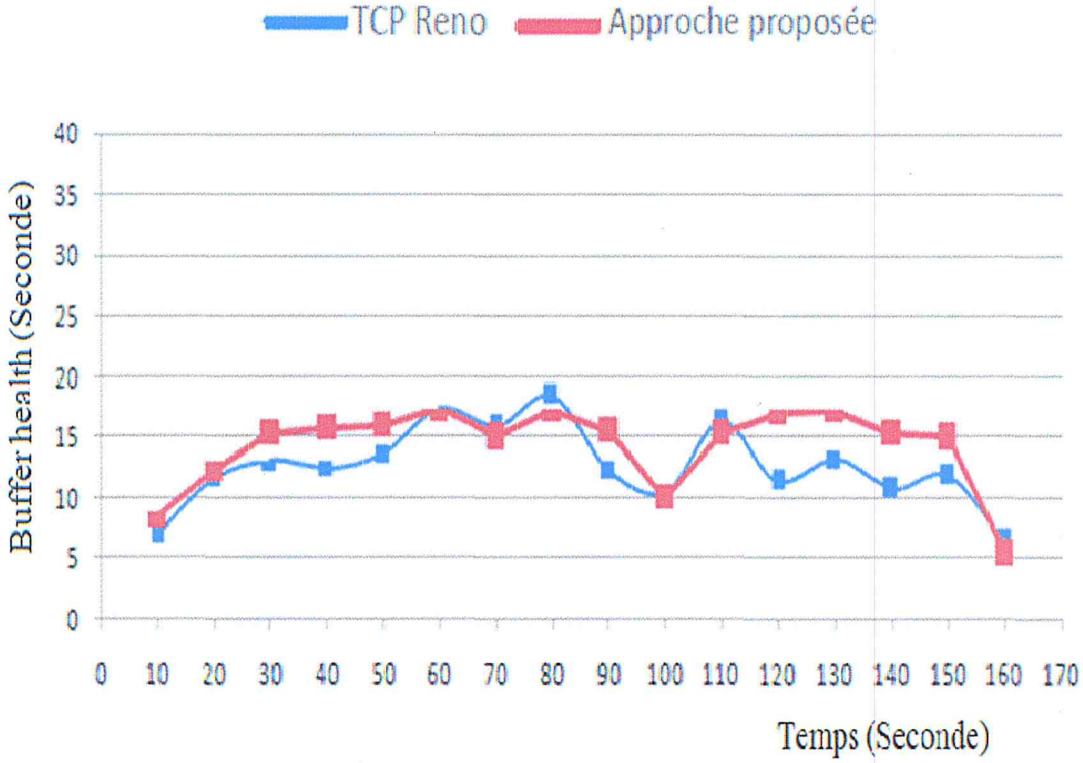

Figure 29 : le résultat du buffer health dans la distance 14 m

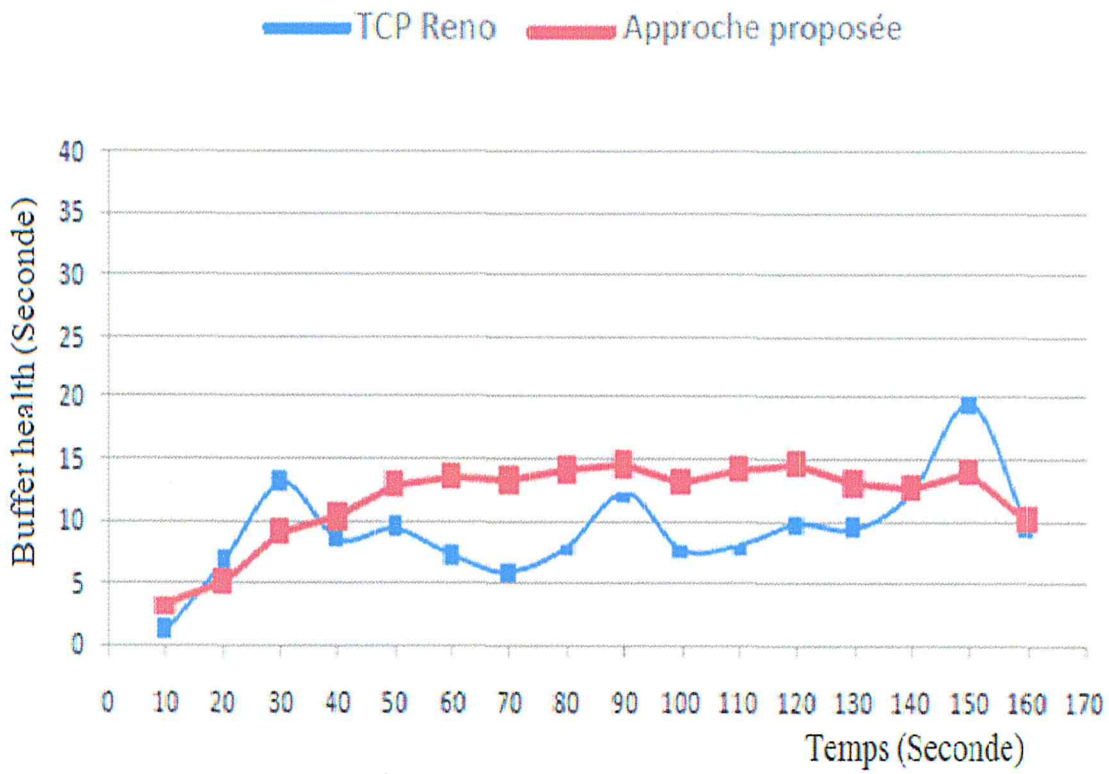

Figure 30 : le résultat du buffer health dans la distance 15.5 m

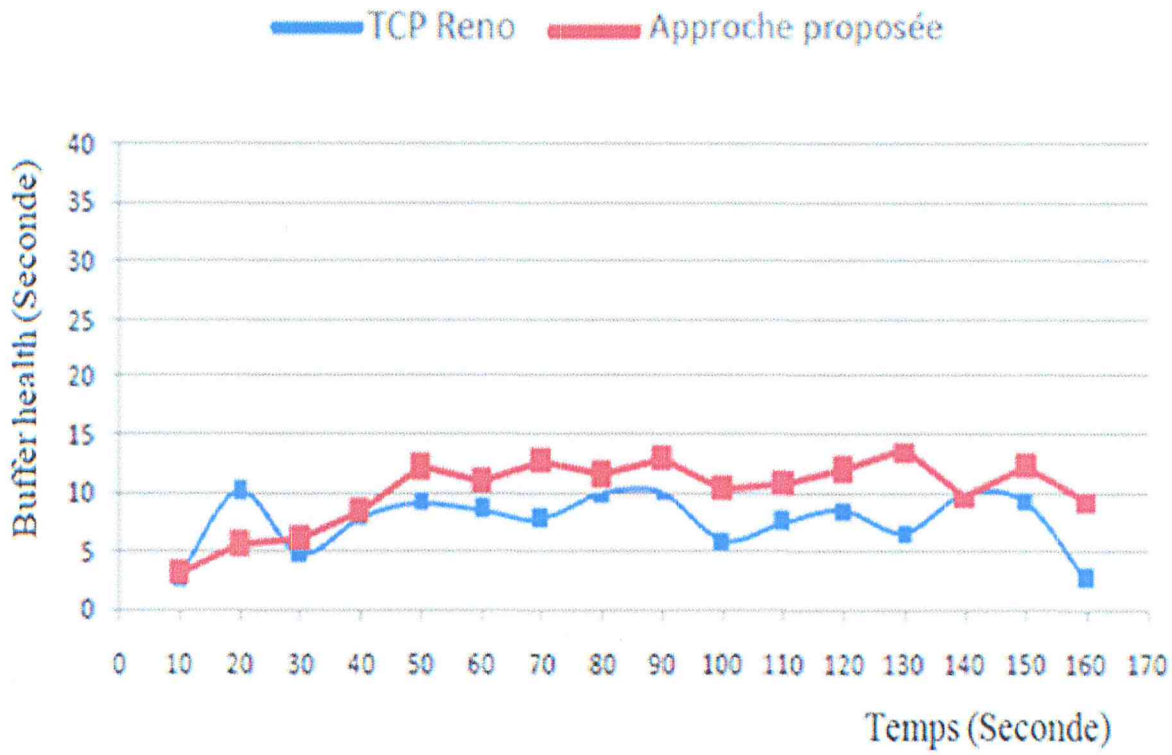

Figure 31 : le résultat du buffer health dans la distance 17 m

4.2 Interprétation :

D'après les figure 26, 27, 28 (dans les deux cas), nous avons noté que lorsqu'on change de distance tout en regardant la même vidéo, la variation du chargement du buffer health avec les deux versions TCP est presque la mêmes. La puissance du signal est bonne car les deux nœuds sont proches. Dans ce cas et en cas de perte de paquet notre approche déduira qu'elle a été provoqué par une congestion du réseau donc elle active le mécanisme de réduction de la fenêtre de flux de TCP (TCP window scaling = 1) afin de traiter les pertes qui sont due à la congestion.

Les figures 29, 30, 31 montrent qu'avec les mêmes paramètres, on remarque que la variation du chargement du buffer health est différentes pour les deux versions de TCP, ceci se remarque d'une façon très importante dans la figure 31, le chargement du buffer health avec le TCP de Ubuntu est un peu lent par rapport à celui de notre approche. Ceci est due au fait que notre approche désactive la fenêtre de flux de TCP (TCP window scaling = 0) lorsque le signal est bas pour mieux traiter les pertes de paquets et ne pas les confondre avec les cas de congestion.

5. Conclusion :

Nous avons proposé une nouvelle adaptation de TCP dans les réseaux sans fil AD HOC. Cette adaptation a été testée dans environnement de vidéo streaming adaptatif. Elle a été validée par l'émulation, les résultats ont démontré l'efficacité de notre approche par rapport aux services existants.

Conclusion général et perspective:

Dans notre travail nous avons proposé une contribution qui vise à améliorer les performances du protocole TCP dans les réseaux sans fil. Pour commencer, on a introduit un axe de recherche et formuler ce problème. Ensuite on a mentionné et défini les généralités qui concerne cette axe afin d'enrichir les connaissances des lecteurs dans le domaine et mieux les aider à comprendre la suite du mémoire. Suite à cela, on a commencé la partie de l'état de l'art ou on a cité, critiqué et comparé les travaux qui existaient auparavant sur notre problématique. Cette partie nous a permis de trouver ce qui manque dans les approches qui existent et de définir nos buts.Une fois nos buts fixés, on a proposé d'implémenter la solution [54] dans le cas réel d'émulation, qui vise à estimer va valeur de puissance de signal du prochain paquet au lieu de la récupérer directement en utilisant la simulation. En cas de perte de paquets, cette valeur vu aider le mécanisme de perte de paquets de TCP àfaire la distinction entre les pertes dues à la congestion et ceux dues à l'environnement sans fil (mobilité),afin de prendre un mécanisme pour d'améliorer les performances de TCP dans les réseaux sans fil.

Les résultats obtenus suite à l'émulation de notre approche ont très bien répondu à nos attentes, les pertes de paquets dusà l'environnement sans fil ont été bien gérées et TCP a pu partiellement distinguer des pertes due à la congestion de ceux qui sont dues à l'environnement sans fil.

Un des inconvenantsmajeur de notre solution est la vitesse des nœuds, qui est fixé à la vitesse de déplacement d'un être humain. Cette vitesse est la base sur laquelle on a choisi un intervalle de calcul de trois secondes.

Afin mieux d'améliorer notre solution on prévoit de rendre la valeur de l'intervalle dynamique en se basant sur les cordonnées GPS.

Bibliographie :

[1] Guy Pujolle, les réseaux, Edition 2011, livre ; P : 195-218.

[2] Dean .T (2001). Réseaux Informatique. Edition RYNALD GOULET

[3] Neil Briscoe, Understanding the OSI 7-Layer Model, Tutorial:Overview.

[4] www.iso.org

[5] Lazard, E. (2006). *Architecture de l'ordinateur*. Pearson Education France.p :92

[6] Edgar H. Callaway, Wireless Sensor Networks: Architectures and Protocols, CRC Press, ISBN: 0849318238, 2004.

[7] Réseaux locaux industriels, ARNATRONIC PLUS, Novembre 2002.

[8] Mattbew S. Gast, 802.11 Wireless Networks: The Definitive Guide, O'Reilly, and ISBN: 0 596-00183-5, April 2002.

[9] Jim Geier, Wireless LANs Implementing Interoperable Networks, Macmillan Network Architecture & development Series USA, 1999.

[10] Khaldoun Al Agha, Guy Pujolle, Guillaume Viver, Réseaux de mobiles & réseaux sans fil, Edition Eyrolles, 2001.

[11] Roberto Arcomano, Guide pratique du réseau sans-fil, Version française du Wireless Howto, 2000-2002.

[12] Nicolas Montavont, La mobilité dans les réseaux IP, DEA Informatique, Université Louis Pasteur de Strasbourg, 2000/2001.

[13] L.Boithias. Propagation des ondes radioélectriques dans l'environnement terrestre .dunod ,1984

[14] A.Glavieux and M.Joindor. Communication numériques-Introduction .Maison.1996

[15] J.G.Proakekis.Digital communications .Third edition .McGraw-holl international Edition. 1995.

[16] [20] Wu, R. H., Lee, Y. H., Tseng, H. W., Jan, Y. G., & Chuang, M. H. (2008, April). Study of characteristics of RSSI signal. In Industrial Technology, 2008. ICIT 2008. IEEE International Conference on (pp. 1-3). IEEE.

[17] Mezghanni, M. S. (2016). Étude de la fiabilité des communications dans un réseau de capteurs sans-fils appliqué aux mines souterraines (Doctoral dissertation, Université du Québec en Abitibi-Témiscamingue).

[18] F. Tobagiet L. Kleinrock, "Packet switching in radio channels: Part ii - the hidden terminal problem in Carrier Sense Multiple-Access modes and the busy-tone solution," dans IEEE Transactions on Networking, vol. 23, no. 12, pp. 1417–1433.

[19] J-F Chambon, Réseaux sans fil, Ecole Nationale Supérieure des Mines, Saint Etienne, janvier 2005.

[20] Q.WANG AND W.YANG. Energy Consumption Model for Power Management in Wireless Sensor Networks. 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2007

[21] M. Gwendal Le Grand, Thèse de doctorat, Qualité de service dans des environnements Internet mobile, Université Pierre et Marie Curie, Juillet 2001.

[22] Michaël Hauspie, Mémoire de DEA, Spécification et implémentation de la couche de communication sans fil pour Objets Mobiles Communicants, Laboratoire d'Informatique Fondamentale de Lille, juillet 2001.

[23] Cyber Networks, Livre Blanc Sécurité des sans fil, janvier 2004.

[25] Houda Labiod, Étude sur le WiFi pour le Conseil stratégique des technologies de l'information (CSTI), septembre 2002.

[25] www.wi-fi.org

[26] Santi, Paolo, Topology Control in Wireless Ad Hoc and Sensor Networks, John Wiley & Sons Ltd, ISBN-13: 978-0-470-09453-2, ISBN-10: 0-470-09453-2, 2005.

[27] Jérôme Herbillon et Daniel Gartner, WiMAX, WRAN, WiMobile, WiMédia, MiMo, Zigbee, Décembre 2005.

[28] Martin De Wulf, Un logiciel d'illustration des protocoles GSM et GPRS sur la voie radio, Mémoire présenté pour l'obtention du grade de maître en informatique, Facultés Universitaires Notre-Dame de la Paix, 2000-2001.

[29] GPRS General Packet Radio Service, White Paper by Usha Communications Technology, June 2000.

[30] A. S. HELAL, B. HASKELL, J. L. CARTER, R. BRICE, D. WOELK et M. RUSINKIEWICZ, Any Time, Anywhere Computing, Kluwer Academic Publishers, 1999, http ://www.wkap.nl

[31] S. CORSON et J. MACKER, Mobile Ad hoc Networking (MANET) : Routing Protocol Performance Issues and Evaluation Considerations, Request For Comments (RFC) 2501, janvier 1999, statut : « Informational »,http ://www.ietf.org/rfc/rfc2501.txt.

[32] J. Postel, "Transmission Control Protocol", RFC 793, IETF, September 1981.

[33] Savo G. Glisic, Advanced Wireless Networks 4G, University of Oulu, Finland John Wiley & Sons, 2006.

[34] Allman M., Paxson V., Stevens W., TCP Congestion Control, RFC 2581. s.l.: IETF Network Working Group, Avril 1999.

[35] P. Karn, C. Partridge, Estimating Round-Trip Times in Reliable Transport Protocols, in Proceedings SIGCOMM '87, Stowe, VT, Aout 1987

[36] D. Cormer. TCP/IP: Architecture, Protocols, Applications. Inter-editions, 1992.

[37] Allman M., Paxson V., Stevens W., « TCP Congestion Control », RFC 2581,Avril 1999.

[38] K. J. K. and Ross, Computer Networking - A top-down approach featuring the Internet.Addison-Wesley, 2003.

[39] K.K. Ramakrishnan, D.M. Chiu, R. Jain, "Congestion Avoidance in Computer Networks with a connectionless Network Layer", Technical Report DEC-TR-509, Digital Equipment Corporation, 1987.

[40] D. Chiu, R. Jain, "Analysis of the Increase and Decrease Algorithms for Congestion Avoidance in Computer Networks," in Computer Networks and ISDN Systems, 17:1-14, 1989.

[41] Jacobson, V., Modified TCP congestion avoidance algorithm. Technical Report 30, April 1990. ftp://ftp.ee.lbl.gov/email/vanj.90apr30.txt.

[42] V. Jacobson, "Congestion avoidance and Control", SIGCOMM symposium on Communications Architectures and Protocols, pages 314-329, 1988.

[43] V. Jacobson, "Berkeley TCP Evolution from 4.3 Tahoe to 4.3 Reno," Proceedings of the 18th Internet Engineering Task Force, University of British Colombia, Vancouver, BC, Septembre 1990.

[44] L.S. Brakmo, S. W.O'Malley, L.L. Peterson, "TCP Vegas: New techniques for congestion detection and avoidance," in Proceedings of ACM SIGCOMM'94, pp. 24-35, Octobre 1994.

[45] Larry Peterson LiminWang Steven Low. Understanding tcp vegas : A duality model. 2000.

[46] K. Fall, S. Floyd, "Simulation-based Comparisons of Tahoe, Reno and SackTCP", in Computer Communication Review, vol. 26, pp. 5--21, July 1996.

[47] M. Mathis, J. Mahdavi, S. Floyd, A. Romanow, "TCP Selective Acknowledgement option," RFC 2018 IETF, Octobre 1996.

[48] V. Jacobson, "Compressing tcp/ip headers for low-speed serial links," 1990.

[49] B. Bakshi, P. Krishna, N. H. Vaidya, and D. K. Pradhan, "Improving performance of tcp over wireless networks," in in Proceedings of 17th International Conference on, pp. 365–373, 1997.

[50] J. L. Sun and S. Singh, "Atcp: Tcp for mobile ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 19, pp. 1300–1315, 1999.

[51] G. B. C. P. Subir, Kumar Sarkar; T, Ad hoc Mobile Wireless Networks. Auerbach Publications, 2007.

[52] G. HOLLAND, N. H. VAIDYA, Analysis of TCP Performance over Mobile Ad Hoc Networks, Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'99), pages 219-230, Washington, USA, Aout 1999,

[53] F. Klemm, Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "Improving tcp performance in ad hoc networks using signal strength based link management," Ad Hoc Netw., vol. 3, pp. 175–191,March2005.[Online]. Available: http://dl.acm.org/citation.cfm?id=1640913.1640956

[54] D.Yassine, « Amélioration de la performance de TCP dans les réseaux mobiles ad hoc », IEEE proceeding SACONET, Paris, 2013.

[55] Chatty, S., Boulabiar, M. I., & Tissoires, B. (2011, May). L'évolution de Linux vers les nouvelles formes d'ordinateurs personnels. In SETIT 2011: 6th International Conference on the Sciences of Electronics, Technologies of Information and Telecommunications (pp. Article-N).

[56] Maza, W. D. D. (2016, August).A Framework for Generating HTTP Adaptive Streaming Traffic in ns-3. In SIMUTools-9th EAI International Conference on Simulation Tools and Techniques-2016.58.4 (2011): 1154-1161.

[57] Ullah, I., Bonnet, G., Doyen, G., & Gaïti, D. (2011, May). Un classifieur du comportement des utilisateurs dans les applications pair-à-pair de streaming vidéo. In Actes du 16e Colloque Francophone sur l'Ingénierie des Protocoles (pp. 12-p).

[58] S. Bauer, D. D. Clark, and W. Lehr, "The evolution of internet congestion." TPRC, 2009.