الجمـــــهوريـــــة الجـــزائريـــــة الديـــمقراطيـــة الشعبيـــــة
RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
وزارة التعـلـيـــــم العـالـــــي و البـــحث العلـــــــــمي
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
جـــــامعـة عمـــــــار ثليـجي بالأغـــواط
UNIVERSITÉ AMAR TELIDJI LAGHOUAT

كـلـيـــــــة العلـــــــــــــوم
FACULTÉ DES SCIENCES
DÉPARTEMENT DE MATHÉMATIQUES ET INFORMATIQUE

MÉMOIRE DE MASTER

DOMAINE : MATHÉMATIQUES ET INFORMATIQUE **(MI)**
FILIÈRE : INFORMATIQUE
OPTION. : RÉSEAUX, SYSTÈMES ET APPLICATIONS RÉPARTIS **(ReSar)**

Présenté par :
Biaa Mohamed

Thème :

Evaluation des performances du protocole SCTP dans les réseaux VANETs

Soutenu publiquement devant le jury composé de :

M.B. YAGOUBI	Maître de Conférences	U. Laghouat (Président)
Mlle. S.BENKOUIDER	Maître-assistant	U. Laghouat(Examinateur)
Mlle. F.Z.BOUSBAA	Maître-assistant	U. Laghouat (Examinateur)
N.LAGRAA	Maître de Conférences	U. Laghouat (Rapporteur)

ANNÉE UNIVERSITAIRE 2011/2012

L'analyse de performance du protocole TCP dans les réseaux VANets

Mohamed BIAA

15 juin 2012

Dedicace

A mes parents

Remerciements

Au terme de ce travail nous tenons à remercier en premier lieu
" ALLAH" qui nous a donnaé la force pour mener à bien l'étude
de ce travail.
Je tiens à exprimer mes sincères remerciements à mon encadreur
Mr. Nasreddine LAGRAA, Maître de conférences à l'université
de Laghouat, Pour leur aide sans limite et leur précieux conseil
qu'il m'a donnés, et qui était pour moi un immense honneur de
travailler avec lui durant le travail dans ce mémoire,
Je remercie aussi mes enseignants, mes collègues, mes amis et
toutes les personnes qui m'ont aidé durant mon étude universitaire.
Et finalement nous sommes trés reconnaissants de l'aide et des conseils
de tout ce qui ont contribué directement et indirectement à la réalisation de
ce travail.

Résumé

Le protocole de la couche transport TCP traite la perte des paquets dans les réseaux filaires comme une congestion du réseau, mais, dans les réseaux sans fil ou mobiles, les pertes peuvent se produire généralement à cause des conditions liées au support de transmission. Donc, la résolution des défis liés au canal de transmission est une tâche indispensable pour assurer une connexion fiable et efficace entre les réseaux filaires et sans fil toutes en adaptant ou développant un protocole de bout en bout. Malheureusement, dans les réseaux VANet, on ne peut pas appliquer directement les protocoles existant pour les réseaux mobiles, car le défi est plus grand à cause de la forte mobilité des nœuds. Dans ce mémoire, on a présenté de façon détaillée les principaux protocoles de la couche transport développés pour le contexte de chaque type de réseau. Ensuite on a analysé par simulations l'un de ces protocoles (SCTP) dans un environnement véhiculaire en comparant ses performances avec celles du TCP standard.

Abstract

The TCP transport layer protocol analyze the packet loss in the wireline networks such as network congestion, but in wireless or mobile networks, losses may generally occur due to the transmission support conditions. Therefore, the resolution of the challenges linked to the transmission channel is a necessary task by adapting or developing a protocol from end to end to ensure a reliable and efficient connection between wired and wireless networks,. Unfortunately, the MANET protocols can not be directly applied in VANet, because the challenge is greater due to the high mobility of nodes. In this brief, the principals of transport layer protocols developed for the context of each type of network was presented in detail. Then we analyzed by simulations one of these protocols which is SCTP in a vehicular environment by comparing its performance with those of the standard TCP.

Table des matières

Table des figures

Chapitre 1

Introduction générale

Les systèmes de transport intelligent (ITS) sont considérés depuis plusieurs années comme un sujet d'actualité qui attire de plus en plus la communauté de recherche et celle des industries (automobiles, télécommunications, etc.). Dans de tels systèmes, les communications inter-véhiculaires sont devenues une composante essentielle pour la mise en œuvre et l'amélioration des performances globale en termes de sécurité ou de confort.

Ainsi, les applications développées pour améliorer la sécurité des individus, réduire les congestions et les embouteillages ou limiter l'impact des véhicules sur l'environnement,... etc ; sont généralement implémentées dans les couches réseaux inférieures -Mac par exemple- vu qu'elles nécessitent un délai très court.

Tant que les applications visant à augmenter le confort des passagers en leurs permettant d'accéder à Internet, de télécharger des fichiers ou de jouer en réseau,... etc, sont généralement des applications implémentées dans les couches supérieures, et ont des exigences sur la fiabilité. Ces applications ne peuvent pas être mis en œuvre sans l'utilisation d'un protocole fiable de la couche transport.

Le protocole TCP par exemple a été initialement développé pour une connexion câblée à haute vitesse où les bandes passantes sont larges et le temps d'attente est très petit. Le protocole TCP exige aussi l'envoi d'un accusé de réception rapide pour chaque paquet envoyé sinon, un " time out " sera déclenché et le paquet sera retransmis. Ce problème peut atteindre des proportions exponentielles lorsque plusieurs paquets sont retransmis, ce qui rend ce protocole très difficile à utiliser dans un environnement sans fil où les taux d'erreurs sont très élevés.

Donc, tous les protocoles de transport proposés pour les réseaux filaires ne sont pas -malheureusement- adaptés aux réseaux sans fil ou ad hoc. En plus, les protocoles proposés pour les réseaux mobiles comme Indirect TCP (I-TCP), WESTWOOD, TCP-ELFN, Ad-Hoc TCP (ATCP) ne peuvent pas eux aussi appliqués au VANet à cause des caractéristiques spécifiques de ces réseaux tel que la forte mobilité.

Dans ce mémoire, nous nous intéressons à l'étude des performances du protocole TCP dans les réseaux ad hoc véhiculaires et la possibilité de son adaptation.

Ce mémoire contient trois chapitres : le premier est une introduction aux réseaux sans fils et en particuliers aux réseaux véhiculaires, le deuxième chapitre présente une taxonomie des protocoles de la couche transport dans les réseaux filaires, sans fil et Ad hoc.
Et le troisième chapitre est consacré à la présentation de deux protocoles proposés, l'un pour les VANet el le deuxième pour voir comment il doit être adapté pour VANet, et aux résultats de simulations obtenus. Enfin, on termine ce mémoire par une conclusion.

Chapitre 2

Introduction aux réseaux VANet

2.1 Introduction

Le domaine des communications inter-véhicules (IVC) est l'un des domaines de recherche récents, qui intéresse de plus en plus la communauté scientifique, les constructeurs automobiles et les opérateurs des télécommunications. En effet, les systèmes de communication inter-véhicules peuvent être utilisés pour mettre en place plusieurs types d'applications appartenant aux systèmes de transport intelligents (ITS) visant à rendre la route plus sure et de rendre le temps passé sur les routes plus convivial [1].
Afin de répondre á une large classe d'applications ITS, deux types de communication sans fil ont adoptés par ITS [2] : la communication á courte portée et á longue portée.
La communication á longue distance s'appuie principalement sur les réseaux d'infrastructures existantes telles que les réseaux cellulaires.
La communication á courte portée est basée sur les technologies émergentes telles que les variantes 802.11, les réseaux mobiles Ad Hoc MANET (Mobile Ad Hoc Networks).
Les réseaux composés des nœuds mobiles et (ou) des équipements routiers fixes (comme les réseaux Ad hoc Véhiculaires (VANet : Vehicular Ad Hoc Networks) qui nous s'intéressent.
Quand les VANets est un type particulier des réseaux sans fils, alors dans ce premier chapitre, au début on va parler sur les réseaux sans fils en général, et ensuite sur les VANets en particulier(leurs architectures, leurs caractéristiques...).

2.2 Les réseaux sans fils

Un réseau sans fil est un ensemble d'appareils connectés entre eux et qui peuvent s'envoyer et recevoir des données sans qu'aucune connexion « filaire » physique reliant ces différents composants entre eux ne soit nécessaire.
Les réseaux sans fil permettent de relier trés facilement des équipements distants d'une dizaine de mètres à quelques kilomètres.
Selon la zone de couverture géographique offerte par le réseau sans fil, on distingue quatre catégories de réseaux sans fil (cf.Figure 1.1) : réseaux personnels (WPAN), réseaux locaux (WLAN), réseaux métropolitains (WMAN) et réseaux étendus (WWAN) [3].

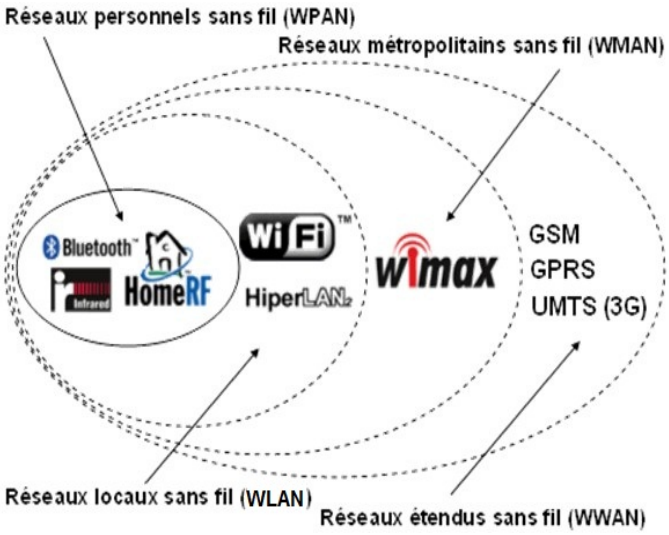

FIGURE 2.1 – Les catégories des réseaux sans fil

La communication dans les réseaux sans fils a deux différentes formes :

2.2.1 Le mode infrastructure

Cette architecture est la plus utilisée. Elle est particulièrement adaptée pour assurer la connectivité dans des lieux précis tels que dans les aéroports et les hôpitaux.
Contrairement au réseau ad hoc où chaque station doit être capable d'effectuer toutes les opérations. Ce mode repose sur un réseau sur lequel un nœud mobile communique uniquement avec un nœud fixe appelé point d'accès, qui est le responsable des services d'authentification et d'association, il

peut jouer aussi le rôle de concentrateur [4]. Cependant, il existe plusieurs environnements d'application des réseaux sans fils (cf.Figure 1.2).

2.2.2 Le mode ad hoc (Indépendant basic service set, IBSS)

Dans le réseau ad hoc, l'infrastructure n'est pas nécessaire d'être déployée préalablement pour permettre la communication entre ses membres.
Chaque station opère de manière autonome afin d'assurer sa connectivité et celle avec les autres membres. La souplesse de déploiement est un atout majeur de ce type des réseaux.
Cette architecture est très utilisée dans les scènes qui nécessitent un déploiement rapide et qui prisent en compte la mobilité des stations.

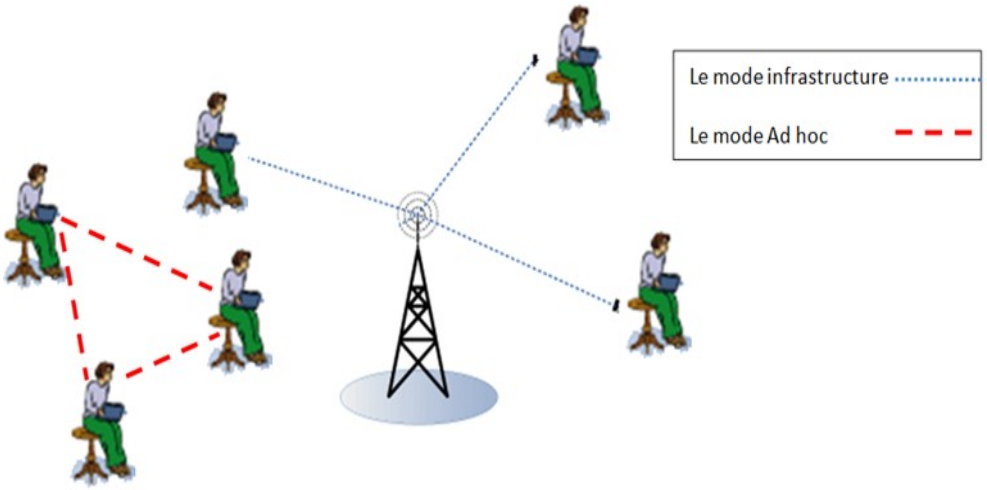

FIGURE 2.2 – Les modes infrastructure et ad-hoc des réseaux sans fils

2.3 Les réseaux ad-hoc véhiculaires -VANet-

Les réseaux VANet (Vehicular Ad Hoc Networks) ne sont qu'une application des réseaux ad hoc mobiles(MANET) où les nœuds représentent les véhicules en déplacement. Ces nœuds sont caractérisés par la forte mobilité des véhicules et la non mobilité des nœuds installés sur les côtés de la route appelés RSU (Road Side Unit).

La communication dans ce type de réseaux peut s'établir à l'aide de plusieurs technologies comme les réseaux sans-fil de type 802.11, WIMAX, Bluetooth... [5], où ces technologies peuvent être installées au sein de véhicules ou sur les RSUs.

Les réseaux VANets peuvent utiliser deux types de communications :

–i) La communication à **un seul saut** aux voitures voisins pour les informer d'un événement (p. ex., le freinage). –ii) à **multi-sauts** pour diffuser des informations ou des requêtes pour un service (cf.Figure 1.3).

2.3.1 Les architectures de communication dans les VANets

On distingue principalement trois architectures de communication [6] : ad-hoc (V2V), avec infrastructure (V2I) et hybride. Dans la première architecture (V2V), les véhicules participants forment un réseau mobile ad hoc pour établir des communications entre les véhicules seulement. Dans ce type de communication, les véhicules peuvent par exemple s'échanger des informations sur leurs positions et leurs vitesses, afin de contrôler le non-respect de la distance de sécurité [7].

La deuxiéme architecture (avec infrastructure) intègre les technologies cellulaires ou autres réseaux véhiculaires où on trouve, V2I (Véhicule à Infrastructure), et I2V (Infrastructure à Véhicule). Ce type de communication peut par exemple être utilisé pour offrir une connexion à Internet aux véhicules via les RSU installés le long des routes qui jouent le rôle des passerelles.

La troisième architecture hybride est une combinaison de deux architectures précédentes qui permet aux véhicules de communiquer entre eux en mode Ad hoc ou avec un point d'accès (RSU) [5].

2.3.2 Les caractéristiques des réseaux VANet

Comme dans les MANETs, la communication dans les VANets est susceptible d'être affectée par plusieurs facteurs [8] :

- La grande vitesse des véhicules.
- La capacité d'énergie et stockage.
- La nécessité d'une sécurisation de l'information.
- Les facteurs d'environnement : obstacles, tunnels, congestion etc...
- Les modèles de mobilité déterminés qui dépendent des conditions de circulation.
- Le problème de rupture de communication (les réseaux isolés des voitures en raison de la fragmentation du réseau).

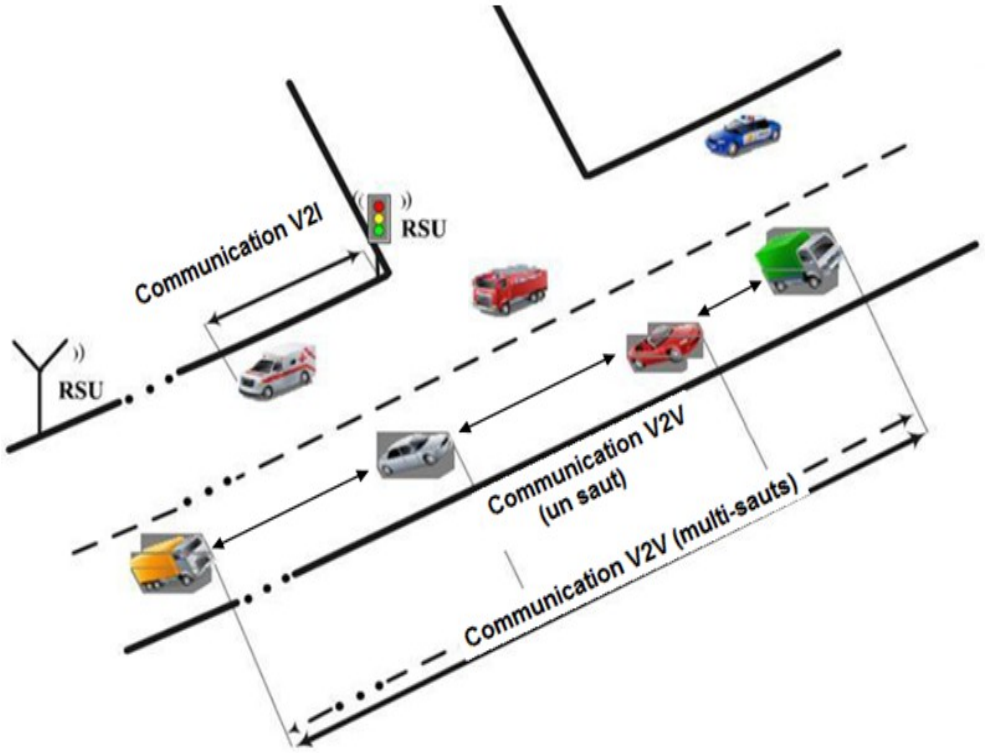

FIGURE 2.3 – Les modes de communications dans les VANets [5]

– Congestion élevée des canaux (p.ex, en raison de forte densité des nœuds)
– La localisation des nœuds change de façon trés rapide et imprévisible.

2.3.3 Les applications des réseaux de véhicules

De nouvelles possibilités et des technologies connexes comme les applications de contrôle des accidents et les mises à jour des conditions météorologiques ont apparues avec VANET.

Les nouveaux systèmes de communication ITS sont étudiés au niveau mondial pour offrir aux passagers des véhicules, garantissant plus de sécurité routière et plus de confort.

La majorité de ces systèmes prévoient l'existence d'une infrastructure de communication fixe installée au bord de la route. Les communications dans les réseaux véhiculaires varient selon le type d'architecture utilisée. Généralement les applications ITS, sont classées en quatre catégories selon [1] :

–i) applications orientées aux infrastructures afin d'optimiser leur gestion (gestion des autoroutes, transport de marchandises, organisation des urgences

etc...).

–ii) applications orientées aux véhicules afin d'améliorer la sécurité routiére (alertes accidents, prévention des carambolages, conduite assistée etc...).

–iii) applications orientées aux conducteurs afin de faciliter l'usage de la route (signalisation dynamique pour les travaux, estimation en temps réelle du meilleur trajet, etc..).

–iv) applications orientées aux passagers pour offrir des nouveaux services à bord de la voiture (accès internet, jeux distribués, messagerie instantanée, informations touristiques etc...).

Concernant les VANets, on peut classer les services offerts en deux autres classes principales :

- **La première classe** comporte les applications de sécurité routière qui visent à améliorer le niveau de sécurité dans les routes, Dans ce cas, les VANets peuvent être vus comme un complément [8] pour le système de transportation intelligent courant. Comme exemples de ces applications on a : La dissémination des messages d'alerte en cas d'accidents, les avertissements de collision des véhicules, et le non-respect de la distance de sécurité.
- **La deuxième classe** comporte les applications de confort qui peuvent être utilisées par les passagers comme l'accès à Internet, la messagerie instantanée, les jeux en réseaux et même pour les conducteurs comme la gestion des espaces libres dans les parkings, les applications dans cette classe contiennent aussi les services commerciaux.

Les contraintes de ces applications sont différentes comme (vitesse de propagation de l'information, bande passante,etc...). Dans le cas d'un accident par exemple, il faut prévenir les usagers dans le minimum de temps, tant que pour diffuser une publicité il faut une large bande passante sans se préoccuper de temps de diffusion.

3.3.1 Exemples d'application :

évitement de collision (carambolage) :

L'objectif principal de cette application est d'éviter les collisions. Ce type d'applications de sécurité sera déclenché automatiquement lorsqu'il y a une possibilité de collisions entre les véhicules, à la détection d'une situation de collision possible, les véhicules envoient des messages d'avertissement pour alerter les conducteurs s'approchant de la zone de collision (cf.Figure 1.4) Les conducteurs peuvent prendre les actions appropriées ou le véhicule lui-même peut arrêter ou réduire la vitesse automatiquement.

L'évitement de collision coopérative dans les intersections (ECCI) : Ce type d'applications sera utilisé afin d'éviter des collisions aux intersections. Principalement, un RSU, installé à l'intersection périodiquement distribue l'état de l'intersection des véhicules qui s'approchent. L'information distribuée comprend :

- L'état du signal de trafic (p.ex., rouge, vert, jaune).
- L'état des véhicules approchant de l'intersection qui sont à une distance époque depuis l'intersection (p.ex. emplacement, la vitesse et ainsi de suite).
- Les conditions environnementales de l'intersection (p.ex., météo, visibilité, surface de la route à l'intersection et ainsi de suite).

Les péages électroniques : En utilisant ce service, le paiement se fait via le réseau au lieu de s'arrêter et de régler le paiement.

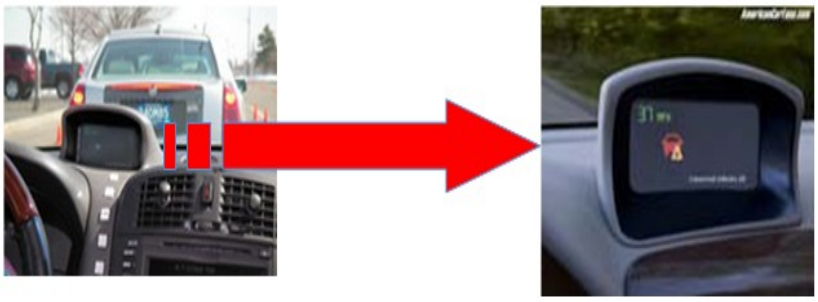

FIGURE 2.4 – exemple d'application d'évitement de collision

2.4 Les technologies utilisées dans les réseaux VANet

2.4.1 DSRC (Dedicated Short Range Communications)

DSRC est une technologie émergeante développée basée sur les normes WiFi définie pour les réseaux dynamiques à forte mobilité [9].
Dans les états unis la commission fédéral de communications (the Federal Communications Commission) a alloué au DSRC la bande 5,9 GHz dans des environnements de communication V2V et V2I. La bande des 5,9 GHz (5.850-5,925) est divisée en sept canaux de 10 MHz non chevauchantes comme illustré dans la Figure 1.5, Un canal est appelé le canal de contrôle, et les six autres sont appelés canaux de service. Certain canaux sont réservés pour un

usage futur. (cf.Figure 1.5). Le canal de contrôle est utilisé afin de diffuser les données de sécurité comme les messages d'avertissement. Il peut également être utilisé pour envoyer des publicités sur les services disponibles, qui peuvent être transférés sur les canaux de service. Les canaux de service sont utilisés pour l'échange de données de façon générale, comme les annonces sur les ventes à proximité des centres commerciaux, téléchargement audio/vidéo, etc...

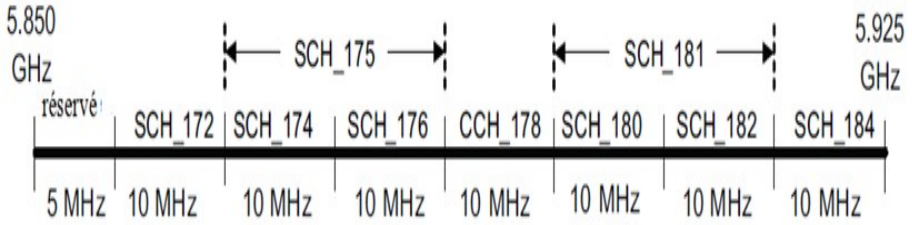

FIGURE 2.5 – les chaines du DSRC [10]

2.4.2 WAVE (Wireless Access in Vehicular Environnement)

Beaucoup d'efforts ont été faits pour concevoir des nouvelles normes liées aux services et aux interfaces pour VANet. Ces normes forment la base pour plusieurs applications dans les environnements des réseaux véhiculaires. IEEE introduit une pile protocolaire complémentaire de la famille 1609 qui a été nommée WAVE. L'architecture de WAVE est développée en basant sur les normes IEEE 802.11p et IEEE 1609 (cf.Figure 1.6) où WAVE integre beaucoup d'amélioration dans 802,11 pour garantir l'échange rapide et fiable des messages de sécutité L'IEEE 802.11p définit les techniques de la couche physique et La couche de Contrôle d'Accès au médium MAC (Media Access Control), alors que l'IEEE 1609 définit les protocoles des couches hautes [9].

La pile protocolaire IEEE 1609

Les standards de famille IEEE 1609 pour WAVE

L'IEEE a défini quatre standards (cf.Figure 1.7) [9], ces derniers sont utilisés pour :

- **IEEE 1609.1 : la gestion des ressources**
  Ce standard définit les services et les interfaces des applications de gestion des ressources dans WAVE. Il décrit aussi les formats des messages et des réponses, il décrit le format de sauvegarde des donneés qui sera

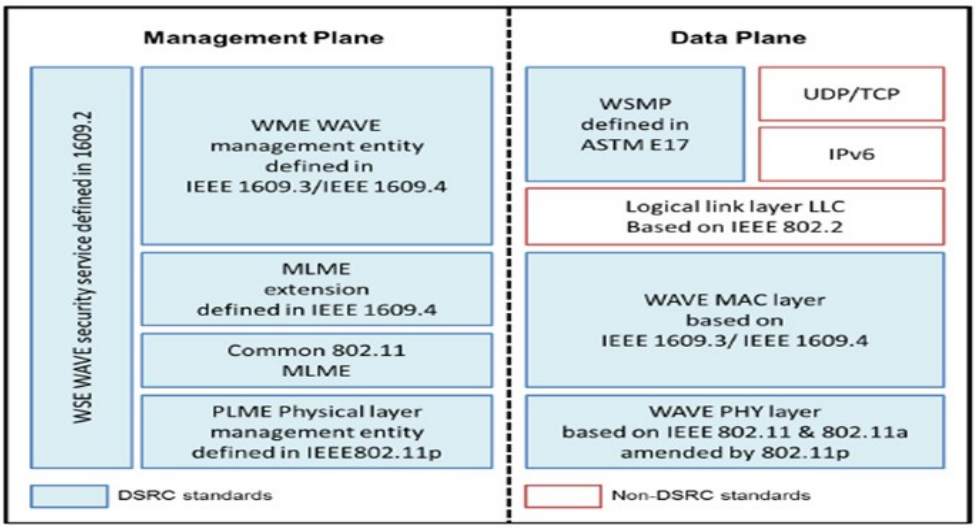

FIGURE 2.6 – la pile de communication DSRC/WAVE [20]

utilisé par les applications pour accéder à d'autres architectures.

- **IEEE 1609.2 : les services de securité**
  Ce standard défini les mécanismes de securité de traitement et de formatage des messages, et les techniques d'échange des messages securisés.

- **IEEE 1609.3 : les services du réseau**
  Ce mécanisme définit les services des couches de routage et de transport, avec la définition des messages specifiques de WAVE pour IPv6 qui peut être supporté par les applications, il définie aussi le MIB (Management Information Base) pour la pile protocolaire.
- **IEEE 1609.4 : les opérations des Multicanaux**
  Ce standard définit les spécifications des multicanaux supportées dans le DSRC.

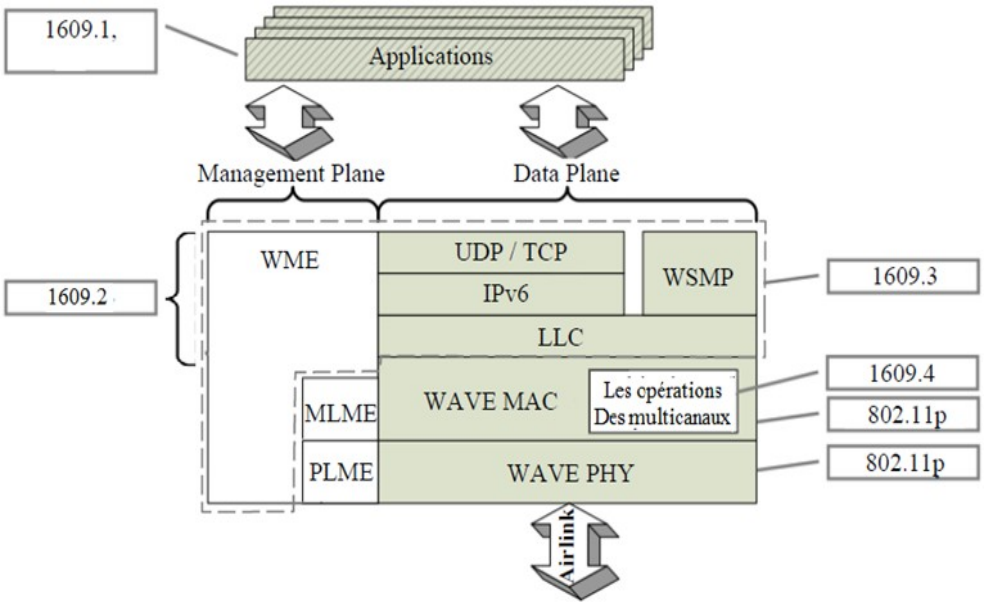

FIGURE 2.7 – la pile protocolaire de WAVE

2.5 Les domaines de recherches dans les VANets

2.5.1 Le contrôle d'accés au medium (MAC) dans les VANet

Différentes techniques de MAC ont été proposées dans la littérature pour VANet. En général, ils sont classés en fonction des probabilités ou du temps.

2.5.2 La dissemination des données dans les VANet

La strategie de transmission intelligente devrait être adoptée afin d'éviter la congestion du canal sans fil.
Les messages de sécurité sont diffusés et devraient être disponibles pour tous les véhicules à l'heure. Par conséquent, les techniques de diffusion devraient réduire au minimum le nombre de retransmissions inutiles pour éviter de surcharger le canal.
Les méthodes de diffusion de données peuvent être classées soit en basant sur l'inondation où chaque nœud retransmet le message reçu, soit en basant sur les techniques d'inondation intelligente (en anglais smart-inondations).

2.5.3 Le routage dans les VANet

Le rôle des protocoles de routage est de déterminer comment transmettre le paquet vers sa destination ?, et comment ajuster le chemin d'accés en cas d'échec ?

Un bon protocole de routage est celui qui a le pouvoir de livrer un paquet dans un temps court avec une consommation de bande passante minimale.

Les protocoles de routage dans les VANet doivent mettre en considération les défis suivants :

- la topologie trés dynamique.

- le partitionnement du réseau : dans les zones rurales, le trafic peut devenir tellement rare qu'on aura des partitions peu dense.

-Les transmissions sensibles au temps : les avertissements de sécurité doivent être transmis aussi rapidement que possible et avec la plus haute priorité.

En général les protocoles sont classés en trois classes principales [10] :

- **Les protocoles proactifs :** comme DSDV et OLSR.
- **Les protocoles réactifs :** comme DSR (Dynamique Source Routing) et AODV (Ad Hoc On-Demand Distance Vector).
- **Les protocoles basés sur la position :** (ou les protocoles de routage géographiques) : comme GPSR.

2.5.4 La localisation

La localisation dans les réseaux VANets constitue l'un des thèmes de recherches les plus importants qui consistent à déterminer la position des véhicules. En effet, un certain nombre de techniques de localisation sont développées et adaptées afin de les utilisés dans VANets tel que Map Matching, Dead Reckoning, Localisation Cellulaire, INS et la localisation par satellites [11].

2.5.5 La sécurité

Dans les réseaux sans fil, le support est partagé. Tout ce qui est transmis et envoyé peut donc être intercepté. Pour permettre aux réseaux sans fil d'avoir un trafic aussi sécurisé que dans les réseaux fixes, le groupe de travail 802.11 a mis au point le protocole WEP (Wired Equivalent Privacy), dont les mécanismes s'appuient sur le chiffrage des données et l'authentification des stations.

la sécurité n'est pas garantie avec le WEP, et un attaquant peut casser les clés de chiffrement sans trop de difficulté.

La Wi-Fi Alliance, l'organisme en charge de la promotion de Wi-Fi, a développé un deuxième mode de protection, le WPA (Wi-Fi Protected Access), qui résout ces problèmes, au moins pour quelques années [3].

2.5.6 La fiabilité des protocoles de couche transport et le multimédia

Dû à la nature de la communication du réseau sans fil, une route peut se casser soudainement. Il est par conséquent important de fournir un service de transport plus fiable que possible.

L'efficacité du protocole de transport est importante pour accomplir la capacité maximale sur les liens sans fil qui sont caractérisés par leurs taux d'erreur élevée, la bande passante variable, et le grand délai.

Dans les deux chapitres suivants on va parler sur les défis d'utilisation des protocoles existants comme TCP dans les réseaux filaires, mobiles et véhiculaires.

2.6 Conclusion

Dans ce chapitre on a présenté tout d'abord les types des architectures dans les réseaux sans fils. Ensuite on a détaillé les concepts liés aux réseaux véhiculaires VANet (ses architectures, ses caractéristiques, ses applications, ses standards DSRC et WAVE, et sur les domaines de recherche).
Dans le deuxième chapitre on va parler du protocole TCP de la couche transport dans les réseaux filaires et les réseaux mobiles classiques.

Chapitre 3

TCP standard et leur défis dans les réseaux sans fils

3.1 Introduction

TCP/IP est né de la réflexion de chercheurs américains suite à un problème posé par l'armée américaine. L'armée américaine disposait de plusieurs bases sur la zone. Chacune de ces bases dispose de sa propre logistique informatique. Les machines des différents centres pouvaient être de types différents et reliées entre elles, à l'intérieur de ces centres par des réseaux locaux différents. Cependant ces centres informatiques doivent échanger des informations. Les bases sont reliées les unes aux autres par des câbles. La question était de trouver un moyen pour que l'information puisse circuler entre ces bases même si certains des chemins empruntables étaient détruits. Il fallut donc trouver un système permettant de retrouver des chemins (routes) qui se reconfigureraient automatiquement en cas de coupures des liaisons. De cette recherche IP (Internet Protocol ou Interconnected Network Protocol) est née, qui permet d'envoyer des informations élémentaires d'une machine à autre machine. Cependant l'information ne part pas d'une machine mais d'une application fonctionnant sur une machine pour aboutir à une application fonctionnant sur une autre machine. Pour résoudre ce problème les chercheurs ont développé un autre protocole nommé TCP (Transport Control Protocol) [12].

3.2 TCP (transport control protocol)

TCP est un protocole de bout en bout (en anglais END to END) de la couche transport. Lorsque deux applicatifs utilisent TCP pour échanger des

données, l'émetteur est sûr que le récepteur reçoit exactement les mêmes données envoyées car TCP gère les contrôles, et la retransmission des paquets en cas d'erreurs.

TCP assure également la remise dans l'ordre des paquets échangés à l'aide des messages d'acquittement envoyés (ACK).

Pour optimiser le transfert, TCP utilise une fenêtre glissante sur le bloc de données qu'il doit envoyer.

TCP est un protocole en mode connecté, car lorsqu'un canal est ouvert entre un client et un serveur, ce dernier reste valide jusqu'à sa fermeture (qui doit être demandé par au moins l'un des deux applicatifs). Pour identifier un service sur la machine distante TCP utilise les ports. Le numéro de port affecté au client par son système d'exploitation est donc réservé durant toute la connexion TCP, que l'applicatif envoie ou non des informations.

3.2.1 Les principales fonctionnalités du protocole TCP

TCP est un protocole de Transport fiable en mode connecté qui fournit des services selon ses caractéristiques, parmi les principales fonctionnalités du protocole TCP il y a :

- L'établissement de connexion qui se fait par la méthode "three way hand shake"
- Transmission point à point, bidirectionnel (entre deux adresses) : (@IP src, port src) –> (@IP dest, port dest)
- TCP traite les données venant des couches supérieures comme une suite d'octets et découpe cette suite d'octets en segments (Taille maximale de 64 Koctets)
- L'application lit/écrit des octets dans un tampon.
- Il assure la délivrance des données en séquence.
- Il contrôle la validité des données reçues.
- Il organise les reprises sur les erreurs ou sur temporisation (la gestion des erreurs).
- Il réalise le contrôle de flux et aussi le contrôle de congestion.

3.2.2 L'entête du protocole TCP

Dans TCP, à chaque flux de données, un entête supplémentaire est ajouté contenant des informations utilisées dans le contrôle de congestion et le contrôle de données. La figure (cf.Figure 2.1) suivante représente l'entête TCP.

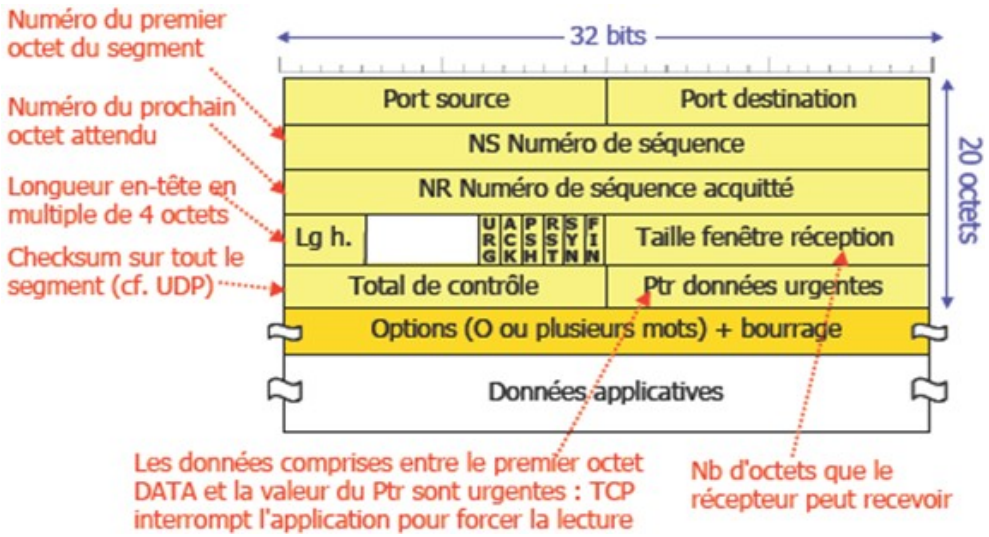

FIGURE 3.1 – L'entête du protocole TCP

3.2.3 L'établissement de connexion dans le protocole TCP

TCP assure la numérotation des paquets, et le destinataire acquise chaque paquet. Il est donc nécessaire pour les deux parties d'établir une négociation du dialogue. C'est pour cela qu'une communication TCP débute toujours par une synchronisation des deux machines. L'émetteur demande au récepteur si ce dernier est prêt à recevoir les données, le récepteur acquise donc la demande, que valide l'émetteur. Les transferts de données peuvent alors commencer (cf.FIGURE 2.2).

3.2.4 Les mécanismes de fonctionnement de TCP

TCP s'appuie sur IP pour gérer le transfert des données entre l'émetteur et le destinataire. TCP fournit également les mécanismes permettant d'établir les connections, de vérifier l'arrivée dans le bon ordre des données, de gérer des données perdues, les erreurs et de récupérer des données concernées. Lors de la transmission de données sous forme de paquet, IP ne vérifiant en aucune maniére que le paquet est bien arrivé, TCP exige que le destinataire envoie un accusé de réception (ACK). De ce fait, l'hôte émetteur peut se trouver devant trois situations différentes :
- Réception d'un ACK : Lorsque le destinataire reçoit un paquet, et si celui ? c'est le paquet attendu.
- Réception d'un NACK : Si la somme de contrôle indique une erreur ou si

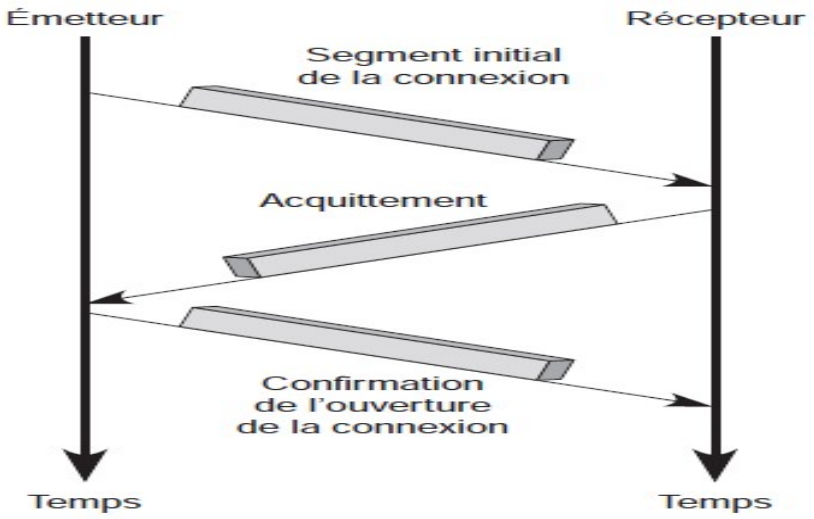

FIGURE 3.2 – L'établissement de la connexion dans TCP

le numéro d'ordre est incorrect.
-Aucune réponse : Si le destinataire ne répond pas, l'émetteur est devant le cas, soit le paquet est perdu, soit la réponse est perdue et il renvoie de ce fait le paquet concerné.

3.2.5 Le contrôle de congestion dans TCP

Internet est un ensemble des réseaux privés et publics, personnels et administrés, interconnecté par l'intermédiaire du protocole TCP/IP.

Si le réseau devient congestionné, aucun personne ne peut utiliser les ressources de réseau et le fait que le réseau est congestionné, les paquets transmis ensuite seraient perdus en raison du manque des ressources telles que les espaces de mémoire tampon dans les routeurs. Alors, les terminaux du réseau best-effort doivent réagir avec les congestions par mise en œuvre du contrôle de congestion afin d'éviter la perte de paquet. Sinon, ils peuvent causer les effets négatifs suivants :

- Augmentation du délai et de la gigue de la transmission de paquets.
- Retransmission de paquet causée par le délai élevé.
- Réduction du débit du réseau et la mal utilisation des ressources du réseau.

L'objectif principal du contrôle de congestion de TCP est de limiter la fréquence d'envoi afin d'éviter de surcharger le réseau lorsqu'il découvre une congestion sur le chemin à destination.

Les fenêtres dans TCP

L'algorithme de contrôle de congestion employé par TCP est basé sur le principe de fenêtres qui sont des espaces de stockage des données limitée par un nombre maximum de paquets. TCP utilise trois types de fenêtres [13] : Fenêtre de congestion (cwnd), fenêtre de réception (rwnd) et fenêtre d'envoie (swnd). La fenêtre de congestion indique la quantité totale de données que peut envoyer l'émetteur est vers le réseau. Tandis que d'autre part la fenêtre de réception indique la quantité de données que le récepteur est prêt à accepter, qui est égale à la taille de tampon disponible sur le récepteur. Et la taille de la fenêtre d'envoi est définie sur le minimum de la fenêtre de congestion et de la fenêtre de réception. On a aussi la notion de Seuil de démarrage lent (ssthresh) qui est l'estimation de la bande passante disponible.

Mécanisme de délai d'attente RTO

Afin d'éviter les longs délais lorsqu'il n'y a aucune réponse du destinataire dans une connexion TCP, un mécanisme de délai d'attente est utilisé. Par conséquent, aprés chaque transmission de segment TCP par un émetteur, un temporisateur est défini et il commence le décompte. Si l'émetteur TCP ne reçoit pas l'ACK avant l'expiration du temporisateur, il suppose que le paquet ou l'ACK est perdu et retransmet le paquet jusqu'à ce qu'un ACK soit reçue. La valeur de délai d'attente (RTO) de retransmission TCP doit être soigneusement choisie.
Si la valeur de la RTO est trop faible, le délai expire rapidement et les délais d'expiration prématurée seront générés au cours de l'opération habituelle de TCP et donc une retransmission inutile aura lieu.
A d'autre part, si la valeur de la RTO est trés grande, TCP réagira lentement à la perte de segment, ce qui signifie le délai de bout-en-bout est plus long qui peut aussi dégrade les performances. Donc, la valeur de la RTO doit être optimisée dans la mesure du possible.

Les phases de démarrage lent et l'évitement de congestion

Les deux phases, démarrage lent et l'évitement de congestion (cf.FIGURE 2.3) ont été introduits par Jacobson. Il permet à l'émetteur TCP de sonder la capacité du réseau en augmentant la fréquence d'envoie. L'algorithme de démarrage lent est utilisé à ce but au début d'un transfert, aprés avoir réparé la perte détecté par le temporisateur de retransmission et aprés les périodes de ralenti, à la réception de données de l'émetteur, le destinataire va acquitter la réception des données de l'émetteur, le récepteur indique effectivement le numéro de séquence du prochain segment de données attendues en ACK. Cela

permet de l'émetteur de conclure que les données de tous les segments qui ont le numéro de séquence inférieur à celui indiqué sont livrés correctement. Alors qu'en cas de perte de paquets, les paquets hors séquence arrivent au récepteur. Le récepteur envoie un ACK en double à l'émetteur dans la réponse de l'arrivée de chaque paquet hors de l'ordre.

La phase de démarrage lent se termine lorsque cwnd atteint un seuil prédéfini " ssthresh " ou quand la congestion est détectée. L'émetteur peut détecter la congestion s'il reçoit trois ACK doublées consécutifs (dupack). Donc on conclut que le paquet est perdu. Le récepteur de données envoie un dupack aprés avoir reçu un segment hors de l'ordre.

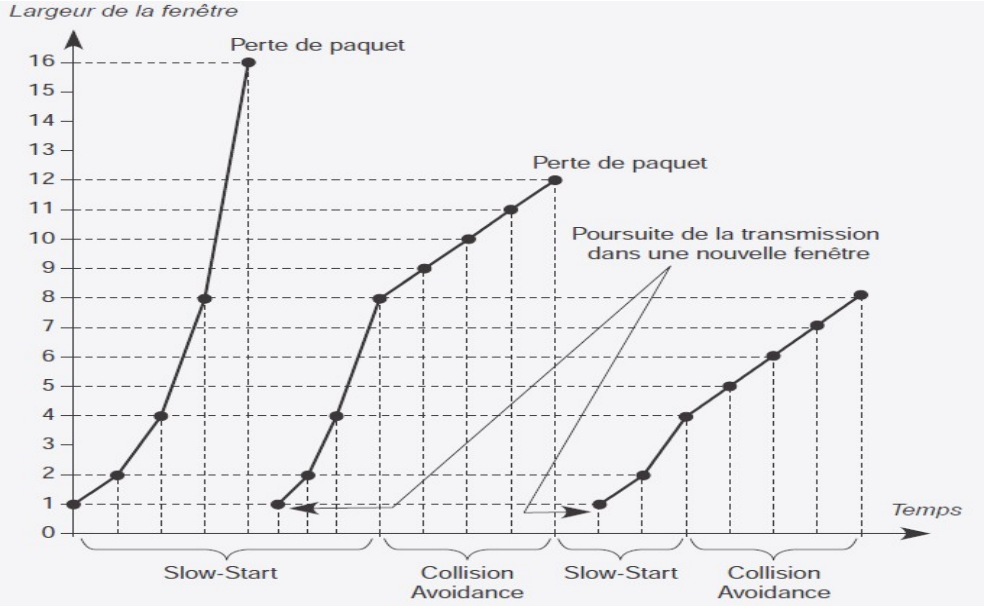

FIGURE 3.3 – Les phases de démarrage lent et l'évitement de congestion[3]

3.2.6 Les variantes du protocole TCP dans Les réseaux filaires

La croissance exponentielle de l'utilisation d'Internet augmente les problèmes de congestion. Par conséquent, de nombreuses versions du protocole TCP existent aujourd'hui (cf.FIGURE 2.4). Actuellement, les principaux types de TCP emploient des algorithmes de contrôle de congestion, démarrage lent(Slow-Start)et d'évitement de congestion et implémente des mécanismes de retransmission rapide de recouvrement [14].

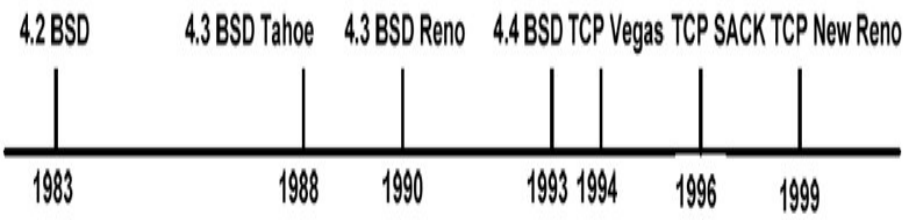

FIGURE 3.4 – Ligne du temps pour les types important du TCP

TCP TAHOE

Dans la premiére version de TCP il n'y a aucun mécanisme de contrôle de congestion, mais aprés l'observation de l'effet de congestion en 1988, Jacobson a introduit plusieurs algorithmes de contrôle de congestion comme TCP-Tahoe. Les algorithmes de contrôle de congestions introduites dans cette version sont les suivants [15] :

- Démarrage lent ;
- Évitement de congestion ;
- Retransmission rapide.

Dans l'algorithme de retransmission rapide, TCP Tahoe retransmet le paquet perdu aprés la réception de trois accusés de réception en double, sans attendre l'expiration du temporisateur de retransmission. Le seuil ssthresh prend par la suite la valeur CWND/2 et le CWND est remis à 1 MSS (Maximum Segment Size). Avant de recommencer la phase de démarrage lent. Plus tard, ils ont trouvé que cet algorithme fonctionne bien en cas de perte d'un seul paquet, mais échoue en cas de perte de paquets multiples dans une fenêtre de données. Chaque retransmission du paquet force TCP Tahoe d'entrer dans la phase de démarrage lent, ce qui entraîne une dégradation importante de la performance. Cette faiblesse du TCP Tahoe est partiellement améliorée en TCP Reno [15] en introduisant l'algorithme de recouvrement rapide.

TCP RENO

TCP Reno introduite une amélioration majeure de TCP Tahoe en modifiant l'action aprés que la découverte d'une perte par ACK doublés. L'idée est de différencier l'action aprés une perte découverte par l'expiration du RTO ou la réception de trois ACK, alors aprés la réception des trois ACKs l'émetteur ne doit pas retourner à la phase de démarrage lent, mais l'émetteur peut continuer la transmission avec réduction de l'utilisation de bande passante. Donc l'algorithme va réduire la valeur de CWND à CWND /2 aprés la retransmission rapide au lieu de 1MSS.

TCP NEW RENO

En cas de pertes multiples, les performances de TCP Reno se dégradent car il ne peut pas éviter les expirations à répétition de temporisateurs. La version TCP New Reno spécifiée modifie légèrement le recouvrement rapide pour prendre en compte les pertes multiples. Dans TCP Reno le premier acquittement partiel stoppe la phase de recouvrement rapide alors que pour New Reno l'acquittement partiel est compris comme une indication de perte : l'émetteur retransmet le premier paquet non acquitté [16].

3.3 TCP dans les réseaux sans fil

TCP est un protocole de transport qui garantit une transmission ordonné et fiable des paquets de données sur les réseaux filaires, mais il fonctionne mal en réseaux sans fil, parce qu'il traite toute perte de paquets sur le réseau comme étant le résultat d'une congestion du réseau et il ralentit sa vitesse de transmission. Cela conduit à une dégradation de la performance.
Le développement des réseaux sans fil, rend nécessaire de trouver des moyens d'améliorer l'efficacité et l'utilisation des ressources de TCP, ainsi que de réduire les temps de latence. Afin de trouver des solutions efficaces à cet effet, les pertes de paquets à travers des liens sans fil devraient être distinguées des pertes de paquets à cause de congestion.

3.3.1 Défis du TCP dans les réseaux mobiles

Contrairement aux réseaux câblés, certaines caractéristiques uniques des réseaux mobiles ad hoc dégradent sérieusement les performances TCP.
Toutes ces caractéristiques posent des grands défis sur TCP pour assurer des communications de bout-en-bout fiables dans les réseaux mobiles ad hoc :

Multi-sauts

Dans les réseaux câblés, les routeurs sont des éléments de réseau distincts qui ont la seule fonctionnalité de routage des paquets. Alors que les réseaux ad hoc sont des réseaux sans infrastructure, donc les nœuds peuvent jouer le rôle des routeurs c'est-à-dire ils sont responsables de l'acheminement des paquets. Et comme inconvénient de cette situation on trouve que le temps aller-retour (RTO) et la probabilité de perte des paquets deviennent grande qui pose une autre contrainte de l'application du TCP dans les réseaux mobiles en général et spécialement dans les réseaux véhiculaires .

La mobilité

Contrairement à un réseau câblé, dans les réseaux ad hoc sans fil, les nœuds sont libres de se déplacer. Ce qui conduit à des changements fréquents de topologie. Alors suivant les auteurs de [17], deux types d'événements sont possibles :

- Perte de chemin d'accès ;
- Partition du réseau.

La perte du chemin mène l'émetteur à trouver un autre chemin, et au cours de cette phase, il n'y aura aucune transmission, ce qui provoque la dégradation de débit. Au cours de cette phase, la recherche d'un chemin peut prendre beaucoup plus de temps que RTO. Donc, le RTO est augmenté de façon exponentielle et TCP va entrer dans la phase de démarrage lent. Cet effet sera plus grave dans l'environnement de haute mobilité comme le cas des réseaux véhiculaires.
En cas de partition de réseau, l'émetteur et le récepteur sont considérés appartenant aux réseaux différents et tous les paquets seront perdus.

L'occupation de canal

Une autre raison de dégradation de performance TCP est l'occupation du canal en raison de l'augmentation de nombre des nœuds et la limitation de la bande passante. Dans IEEE802.11, lorsque le nombre d'essaie d'accès au media partagé dépasse la limite prédéfinie, cela peut causer la perte des paquets et le protocole de contrôle d'accès au media MAC (Medium Access Control) avertit (à tort) la couche supérieure que le chemin d'accès est inaccessible pour que TCP arrête la transmission.

Paquet hors ordre

Lorsqu'un récepteur reçoit les paquets hors ordre, le récepteur transmet ACK doublé. Après avoir reçu trois ACK doublés l'émetteur retransmet les paquets et le contrôle de congestion est activé. Mais le problème c'est que le contrôle de congestion est activé à tort la plupart du temps, parce que la présence de paquets hors ordre ont lieu pour des raisons différentes telles que le protocole de routage multi-chemins et la rupture des liens et pas seulement à cause de congestion.

La déconnexion

les déconnexions peuvent arriver à cause de plusieurs raisons :

- Quand le nœud mobile bouge d'une cellule à une autre. Cette procédure de réassociation, nommée Handover, qui dépend fortement de la technologie de transmission utilisée, peut provoquer de courtes interruptions de la connectivité. Le protocole du transport assimile ces périodes de déconnexion à des phases de congestion et déclenche inutilement la procédure de contrôle de congestion qui diminue le débit du flux
- Quand un hôte mobile bouge de la portée des émetteurs-récepteurs.
- Quand les signaux radio sont bloqués par les bâtiments et d'autres objets semblables.
- Quand une cellule contient un grand nombre d'utilisateurs et la bande passante n'est pas suffisante pour satisfaire leurs besoins.

Toutes ces caractéristiques et d'autres problèmes comme l'interférence et les problèmes des terminaux cachés et exposés ne permettent pas l'application du TCP classique dans ce type de réseaux.
En raison de l'usage commun du TCP dans les applications Internet qui exigent un transfert fiable de données, il est important de garder la pile de protocole TCP/IP et aussi la structure des éléments de réseau comme inchangé que possible, même lorsque les caractéristiques de la mobilité nécessaires à Internet sans fil sont ajoutés au réseau alors TCP doit être modifié afin de satisfaire les attentes de rendement TCP dans le canal sans fil.

3.4 Les travaux connexes

Dans les réseaux mobiles plusieurs études sont faites pour analyser la performance de TCP. La dégradation de performance principalement vient des mécanismes de contrôle de congestion utilisées dans TCP. Par exemple, TCP interprète les erreurs de transmission comme une situation de congestion et donc il réduit la capacité de transmission.
Cependant, les extensions et l'amélioration successive (Tahoe, Reno,...) du TCP ne résolvent pas les problèmes basiques de TCP dans les environnements mobiles.
Pour résoudre ce type de problème, on trouve la notion de connexions séparée (en anglias Split-Connection), L'idée principale derrière les approches de connexion séparé est d'isoler la mobilité et les problèmes liés aux communications sans fils. Cela est reglisé en séparant la connexion TCP entre l'hôte mobile et l'hôte fixe pour avoir deux connexions séparées : une connexion câblée entre l'hôte fixé et la station de base et une connexion sans fil entre la station de base et l'hôte mobile.
De cette manière, la connexion câblée n'a pas besoin de changements dans

le logiciel existant sur les hôtes fixes et la connexion sans fil peut utiliser un protocole mobile spécialisé pour fournir la meilleure performance.
Les protocoles visant à améliorer l'efficacité de communication de bout en bout à la couche de transport peuvent être classés en trois catégories selon [18] :
–i) **les modifications pures de contrôle de congestion**, Marc Bechler, et al dans [18] estiment que la manière évidente pour augmenter la performance est à modifier le contrôle de congestion en TCP. Ils essaient de prévoir à l'avance les situations différentes basées sur les informations locales. Avec l'aide de ces informations, les algorithmes de contrôle de congestion de TCP (comme TCP Vegas et TCP Westwood) sont modifiés pour réagir en conséquence selon les différentes situations.
–ii)**l'utilisation d'information des systèmes intermédiaires**.
A condition que le réseau soit capable à découvrir les situations différentes, le mécanisme commun de la notification de congestion explicite (ECN), où les nœuds intermédiaires sont capables à découvrir des congestions et d'envoyer des alertes qui seront utilisés par TCP pour optimiser l'efficacité de communication.
L'utilisation d'information des systèmes intermédiaires est une approche efficace pour améliorer TCP dans les réseaux mobiles parce que cette information sur le réseau fournit une estimation presque exacte.
Ce concept implicitement prend en compte les notifications, qui activent TCP à réagir rapidement pour plusieurs situations dans le réseau.
Exemple : ATCP (Ad-Hoc TCP)
. iii)**les protocoles de transport complètement nouveaux** .
Cette catégorie contienne les protocoles de transport et que ne sont pas basés sur TCP, comme le Stream Control Transmission Protocol (SCTP).

3.4.1 Exemples de protocoles de transport de la 1ère génération pour les réseaux sans fil à un saut

I-TCP : Indirect TCP

Si un hôte mobile a besoin de communiquer à un autre fixe en utilisant I-TCP, une demande est envoyée à la station de base actuelle pour ouvrir une connexion TCP avec l'hôte fixe de la part de l'hôte mobile.
L'hôte mobile communique avec sa station de base sur une connexion séparée en utilisant une variation de TCP qui est accordé pour les liens sans fil.
Le protocole I-TCP découpe la connexion TCP traditionnelle en deux tronçons séparés par un point intermédiaire (la station de base).

L'I-TCP se compose de deux composantes un sur l'hôte mobile et d'autre

sur la station de base. La composante sur l'hôte mobile se compose des appels de bibliothèque spéciaux qui sont semblables dans la fonctionnalité et l'interface aux appels de socket faits par une application en utilisant TCP classique (standard, régulier), Cette bibliothèque rend la communication nécessaire avec la station de base transparente à l'hôte mobile.

Le protocole I-TCP résidant sur le mobile émet une demande d'établissement de connexion TCP, pour l'utilisateur fixe, à la station de base.
Concernant l'acquittement, un paquet transmis du poste fixe vers le mobile est d'abord acquitté sur le premier tronçon de connexion par la station de base, puis est transmis sur le second tronçon.

La deuxième composante et parmi ses rôles il soutien prend en charge de handover en faveur d'I-TCP.

Les hôtes dans la partie fixe n'ont pas conscience sur les caractéristiques de la partie sans fil.

I-TCP garantit que les erreurs de paquet et les variations de délai sur le lien sans fil n'influent pas sur l'initiation de procédures de contrôle de congestion TCP par l'élimination de la retransmission de bout en bout des paquets qui subissent des erreur à travers le lien sans fil [15].

Parmi les avantages d'I-TCP [19]
- Aucun changement dans le réseau fixe n'est nécessaire.
- Aucun changement pour les hôtes (le protocole de TCP) n'est nécessaire.
- Toutes les optimisations actuelles du TCP fonctionnent sans problème.
- Les erreurs de transmission sur un lien sans fil ne se propagent pas dans le réseau fixe.

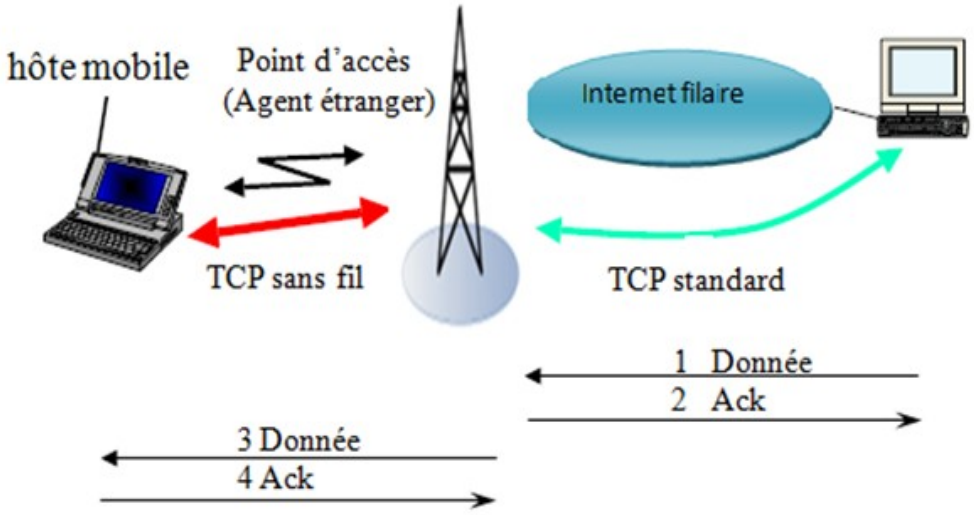

FIGURE 3.5 – le fonctionnement du I-TCP

SNOOP

Le protocole de SNOOP essaie de résoudre le problème de taux d'erreur de bits (BER) de réseaux sans fil en gardant les paquets non acquittées au niveau de la station de base, et en exécutant la retransmission locale sur le lien sans fil pour les paquets perdus. Plus spécifiquement, le protocole de SNOOP présente un agent SNOOP qui réside à la station de base et qui contrôle chaque paquet dans les connexions TCP qui traversent la station de base.

Après les détections de perte des paquets, l'agent de SNOOP retransmet la copie localement cachée cf.FIGURE 2.6.

Cependant, la performance du protocole SNOOP pourrait avoir une dégradée si l'hôte mobile bouge complètement de la couverture de l'ancienne station de base avant que la nouvelle station de base aura le temps de le réassocier le SNOOP des ACK.

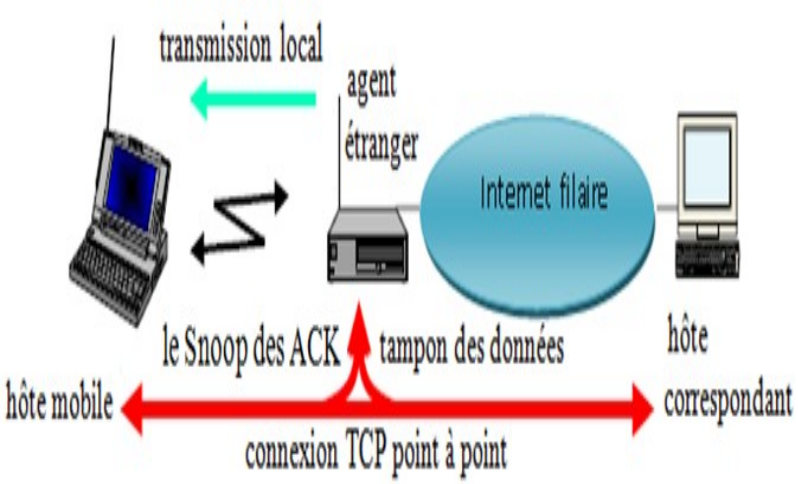

FIGURE 3.6 – le fonctionnement du SNOOP [20]

TCP WESTWOOD

TCP Westwood est une modification de côté de l'émetteur de TCP New Reno en utilisant une technique d'estimation de taux de bout en bout, pour changer seulement l'algorithme d'évitement de congestion tout en gardant la phase du démarrage lent inchangée [15].
L'émetteur TCP, en contrôlant le taux de réception d'ACK, estime continuellement le taux de paquet de la connexion et utilise cette estimation pour déterminer la bande passante disponible.

Quand l'émetteur perçoit que la congestion a apparu, l'expéditeur utilise la bande passante disponible estimée pour ajuster la fenêtre de congestion et les grandeurs de seuil du démarrage lent.

3.4.2 Exemples de protocoles de transport de 2ème génération pour les réseaux sans fil multi sauts

TCP-ELFN et TCP-F [20]

Les protocoles TCP-ELFN (Explicit Link Failure Notification) et TCP-F (TCP-Feedback) sont des propositions faites pour prévenir TCP des " fausses réactions " à des pertes de paquet causées par une rupture de lien.

La rupture fréquente du lien à cause de la mobilité est l'un des facteurs majeurs qui dégradent la performance de TCP.

Tous les deux ELFN et TCP-F s'appuient sur les nœuds intermédiaires pour être informer sur la rupture d'un lien. Dans TCP-F le nœud intermédiaire est sollicité d'annoncer à l'émetteur de TCP un état sur la condition de réseau. Quand un nœud intermédiaire découvre une rupture de lien, il envoie explicitement un avis RFN (route failure notification) à l'émetteur TCP.

La différence entre TCP-F et ELFN à une réponse de la rupture de lien. La ré-établissement de route dans TCP-F est faite après la réception d'un avis (RRN) d'un nœud intermédiaire pour annoncer que ce chemin est soutenu.

Ad-hoc TCP (ATCP)[21]

Il y a beaucoup des solutions de transport existants dans MANET basées sur le partage de l'information à travers plusieurs couches. ATCP (ad hoc TCP) est l'une des approches qui utilisent l'information des notifications ECN et ICMP (destination inaccessible) de la couche de réseau pour estimer et réagir convenablement aux conditions réelle de réseau.

L'idée de cette approche est d'insérer une sous-couche appelée ATCP entre IP et TCP, qui garantit le comportement correct en cas des échecs de route. L'expéditeur TCP peut être mis dans des états comme présentés dans cf.FIGURE 2.7.

En notant qu'à la différence des deux approches précédentes basées sur la réaction, la corruption de paquet provoquée par les erreurs de canal est aussi prise en compte. L'expéditeur peut choisir un état approprié en apprenant les informations d'état de réseau par les notifications de congestion explicite (ECN) et les messages ICMP.

Le diagramme des états de transition pour ATCP à l'expéditeur est montré dans la FIGURE suivante :

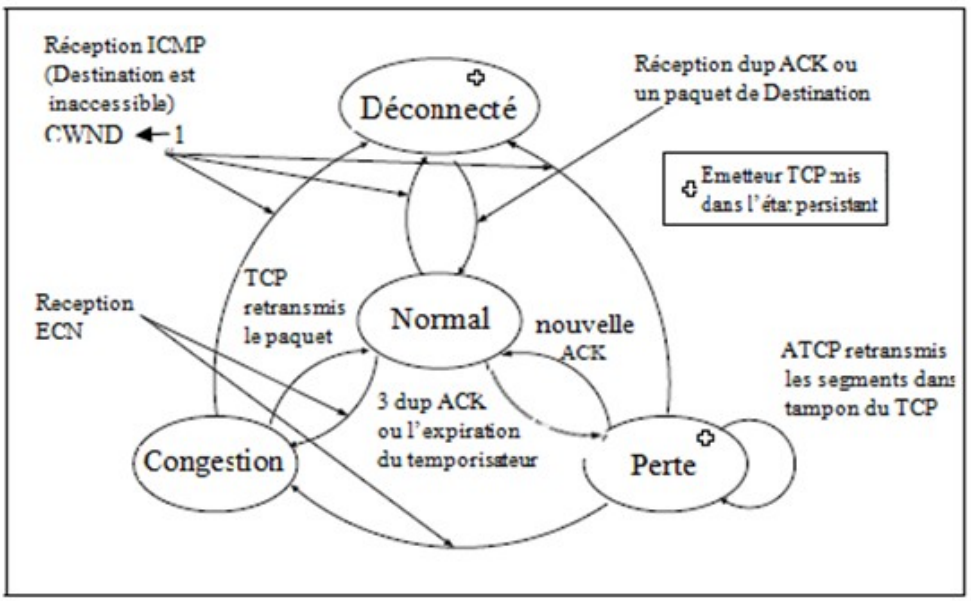

FIGURE 3.7 – diagramme d'état transition pour ATCP [21]

3.5 Conclusion

Dans ce chapitre, on a présenté le protocole de transport TCP, ses principales fonctionnalités et les mécanismes d'évitement de congestion et les algorithmes utilisés puis on a essayé d'expliquer quelques protocoles optimisés et améliorés pour les utilisér dans les réseaux sans fils.
Dans le troisième chapitre on va décrit les améliorations et les développements des protocoles dans les réseaux véhiculaires et les protocoles qui supportent le transfert des multimédia (QoS).

Chapitre 4

TCP dans les réseaux véhiculaire

4.1 Introduction

Le contrôle de la transmission doit être employé pour garantir un niveau de performance souhaité. La conception d'un Transport Control Protocol (TCP) dans VANets est une tâche très difficile [22], car la transmission de données de bout en bout est une transmission sans fils qui caractérisée par les sauts multiples et la forte mobilité.

Afin d'accéder aux services d'Internet, les architectures VANet doivent comporter des proxy, les véhicules vont se connecter à Internet via ces proxies.

un proxy est localisé à une position fixe et peut cacher les caractéristiques des VANet , donc il sépare également la connexion TCP de bout en bout en deux segments entre le proxy et Internet en utilisant TCP classique (standard), et entre les véhicules et le proxy ,en utilisant des protocoles de transport optimisés afin d'améliorer l'efficacité de communication.

4.2 VANet TCP

4.2.1 Le fonctionnement du protocole

En basant sur les connaissances acquises à partir des protocoles ATCP (Ad-hoc TCP) [21] et MCTP (Mobile Control Transport Protocol) [18], un nouveau protocole de couche de transport a été proposé et implémenté par Wantanee Viriyasitavat, et al dans [22] sous le nom de VANet TCP.

Les contributions spécifiques de ce travail sont :

1. la dissimulation du problème de contrôle de transmission de bout-en-bout comme étant un problème de couche réseau (routage).
   L'idée essentielle est d'assurer la stabilité de chaque lien, autant que

possible, ainsi de garantir la stabilité de la route multi-hop. Il est clair que pour certaines applications, la livraison des paquets réussie est plus souhaitable que le fait de pouvoir transmettre un paquet avec le moindre délai. Donc, une route plus stable devrait être choisie même si elle est plus longue.

2. L'utilisation d'une approche de conception inter-couches (cross-layer)dans lequel l'information de la couche de transport est utilisée par la couche réseau afin de permettre la prise des meilleurs décisions par chaque voiture sur une route. Cette flexibilité permet à la couche réseau de choisir dynamiquement une route qui est la plus appropriée pour la couche de transport.
3. Conception d'un nouveau VANet Transport Control Protocol qui permet de détecter les pertes de paquets, d'identifier la cause principale de ces pertes correctement (congestion, la mobilité, conditions de canal sans fil, etc.), et de résoudre ces différents problèmes avec les mécanismes appropriés.

Pour implémenter le VANet TCP, les deux observations suivantes sont prises en compte :

–i) pour les applications insensibles au délai de transmission, où l'état du réseau est l'état normale, la réussite de transmission d'un paquet, même si c'est avec un grand délai, est plus critique que la possibilité de transmettre un paquet avec le plus petit délai, et la plus grande probabilité de perte de paquet.

–ii)Le succès de transmission du paquet devient particulièrement important dans le VANet où les transmissions des paquets sont faites dans un milieu partagé avec des sauts multiples. Il est particulièrement important, car la perte de paquets le long d'une route de n-sauts implique une retransmission de paquets qui doit être fait n fois par la source et des nœuds intermédiaires. Donc, par rapport à la transmission d'un seul paquet, plus de n fois des compétitions sur les canaux et l'utilisation n fois de bande passante sont nécessaires pour chaque paquet perdu ; Et ça donc peut justifier la nécessité d'établir un chemin plus fiable à la couche réseau.

Pour une utilisation maximale de la capacité du réseau (bande passante), une stratégie dynamique est nécessaire pour assurer le compromis entre la probabilité de succès de transmission de paquets et la latence des paquets qui peut changer avec le temps.

La solution proposée dans ce protocole comprend ces composantes principales :

–i)un nouveau protocole de contrôle de transport dans les VANets qui distingue précisément les causes de pertes de paquets et de les traiter d'une

manière appropriée.

–ii) le mécanisme de cross-layer (top-down) qui indique comment et quel type des informations doivent être transmises à partir de la couche de transport à la couche réseau, en utilisant le protocole de routage (BRR) Beacon Reception Rate Routing protocol qui ajuste dynamiquement son processus de sélection de la route sur la base de l'information reçue de la couche de transport.

4.2.2 Description détaillée du protocole

Comme la (cf.FIGURE 3.1) le présente, VANet TCP peut distinguer trois types de perte de paquets :

3.2.2.1 Gestion de perte des paquets

Paquet perdu à cause de la congestion

Modèle de la perte : paquets seront supprimés aléatoirement pendant la période de congestion.

Indication : Réception d'un acquittement ECN-ACK marquée par un bit d'avis de congestion explicite(ECN)

Mécanisme de résolution : Si le système est dans l'état NORMAL il va basculer vers l'état de CONGESTION, et pour chaque ECN-ACK reçu, la couche de transport devrait réduire le débit de transmission (la fenêtre de congestion est réduite par la moitié) avant qu'il continue la transmission des données.

Le système revient à l'état NORMAL s'il reçoit une nouvelle ACK avec un bit d'ECN démarquée (c.-à-d. la congestion a été résolue)

Paquet perdu à cause de la charge du canal sans fil

Modèle de la perte : Les paquets seront supprimés au hasard tout au long de la communication.

Indication : Réception des acquittements doublés.

Mécanisme de résolution : Si le système est à l'état NORMAL, il va basculer vers l'état de CHANNEL LOSS, où il doit sauvegarder le dernier nombre de séquence des paquets transmis, noté par $Seqno_{channel}$. Dans cet état le protocole envoie seulement les segments perdues qui sont indiquées par les ACKs doublées (transmission de toutes les données autorisées par la fenêtre de congestion sans réduction du débit de transmission ou de la taille de la fenêtre de congestion). Le système revient à l'état NORMAL s'il reçoit une nouvelle ACK avec un nombre de séquence plus grand que $Seqno_{channel}$, attestant que tous les paquets perdus ont été recouvrés.

Paquet perdu à cause de déconnexion.

Modèle de la perte : un grand nombre de paquets seront supprimés pendant la période de déconnexion.

Indication : déclenchement de temporisateur des paquets

Mécanisme de résolution : le système va basculer à l'état de DECONNECTION LOSS quelque soit l'état courant. Le système doit sauvegarder les paramètres courants (telle que taille de fenêtre de congestion, RTT etc...), ensuite il arrête la transmission des données et commence à envoyer des paquets périodiques de sonde au réseau jusqu'à qu'une nouvelle route a été découverte.
À la découverte d'une nouvelle route (indiqué par la réception d'ACK), l'état doit basculer à NORMAL en restaurant les valeurs des paramètres sauvés avant la déconnexion.

3.2.2.2 Les Interactions Inter-Couches

Le mécanisme de cross-layer exige dans ce protocole que la couche transport informe la couche de réseau sur la qualité de la route souhaité par elle (cf.FIGURE 3.2).

A l'inverse des approches existantes, le mécanisme utilisé dans cette stratégie est appelé «top-down» dans lequel l'information de la couche de transport est utilisée par la couche réseau pour la prise des décisions par chaque voiture.

L'information utilisée entre la couche de transport et la couche réseau est appelée $EPDR$(t) (expected packet delivery ratio).À la réception de cette valeur, la couche de réseau arrange son processus de sélection d'acheminement, comme le fait le protocole : Beacon Reception Rate (BRR) routing protocol adopté dans ce travail.

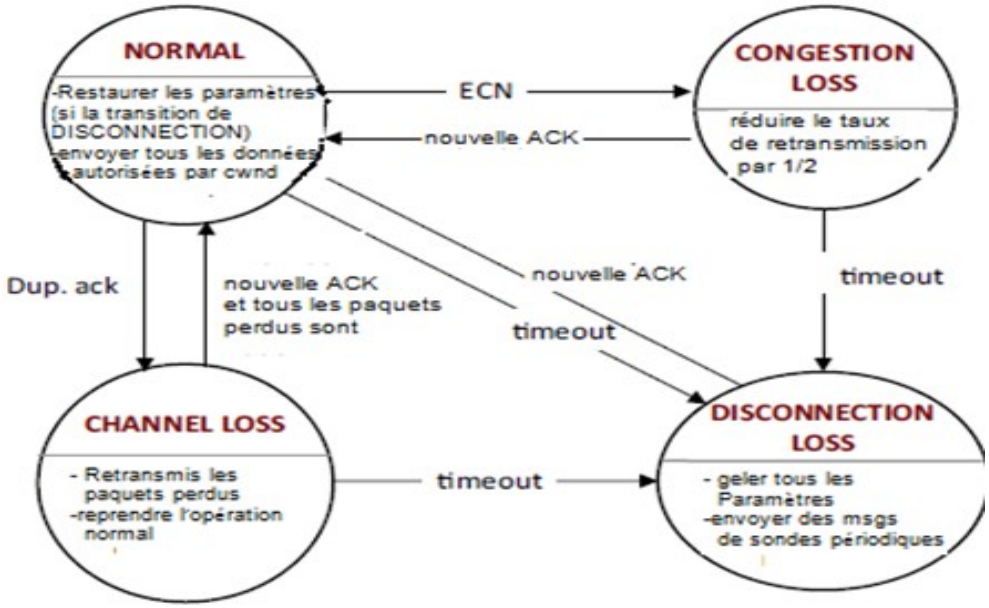

FIGURE 4.1 – diagramme d'état transition pour VANet TCP [22]

Beacon reception rate (BRR) routing protocol

C'est un exemple d'un protocole de routage basant sur la connaissance de l'état de la couche transport-conscient (en anglais transport-aware routing protocol) où il est adopté selon l'information reçue de la couche de transport d'une façon adaptatif et dynamique.
Au lieu de choisir la route avant la transmission de données, le véhicule source et les autres véhicules de relais choisissent un de leurs voisins pour faire suivre le paquet de données vers la destination, Ces dernièrs sont choisis suivant leurs localisations et leurs états de connexion avec le véhicule source et les autres relais.
Dans le protocole de BRR, un véhicule garde en plus de l'adresse et l'information de localisation, la valeur de (BRR) de chacun de ses voisins, Cette information de BRR est utilisée par un véhicule comme indicateur principal pour estimer la qualité de son lien avec voisin et pour déterminer le meilleur relai.

La méthode de calcul de BRR

Le calcul du BRR se fait à des intervalles fixes et connus, le véhicule i peut calculer le BRR de son véhicule voisin J dans le temps T, noté parBRR_i(j, t) de la façon suivante :

$$BRR_i(j,t) = \frac{Nombre\ des\ messages\ recu\ de\ j\ pendant\ [t-w,t]}{Nombre\ des\ messagesmis\ parjpendant[t-w,t]}$$

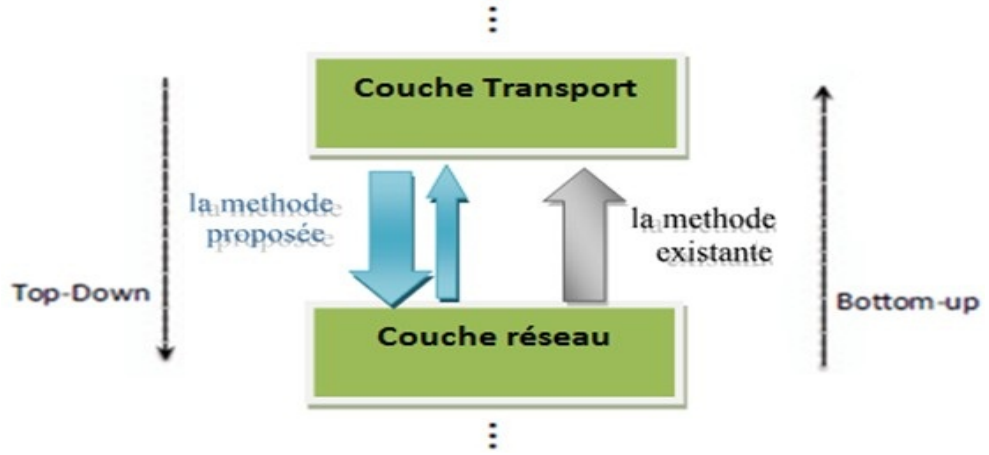

FIGURE 4.2 – la mécanisme de top-down pour les interactions de cross layer

Où le w est la durée de la fenêtre de BRR durant laquelle les statistiques sont rassemblées.

Le choix du prochain véhicule qui va faire transmettre un paquet

En supposant que le véhicule i est le prochain véhicule sélectionné comme l'indique l'entête d'un paquet, alors, si le véhicule i recevra un paquet destiné au véhicule K dans le temps T, va consulter sa table des voisins afin de choisir le prochain véhicule qui doit faire suivre le paquet. S'il y a un véhicule j dit qu'elle est plus approche que i de la destination avec BRR_i(j, t) plus grande qu'un certain seuil noté BRR_i^{th}(j, t) , alors le véhicule j est sélectionné pour être le prochain relais. En revanche, si il n'y aucun bon candidat, le voisin qu'est près de la destination avec le maximum BRR_i(j, t) sera choisi.

Le choix de la valeur du seuil

Le choix est basé sur le rapport calculé de paquet anticipé, PDRe (t), spécifié par la couche de transport, le protocole BRR pour calculer la valeur de BRR_i^{th}(j, t) comme suit :

BRR_i^{th}(j,t)= $PDR_e(t)^{\frac{D_{ij}}{D_{jk}}}$

Où le D_{ij} est la distance entre le véhicule i et J et D_{ik} est la distance entre le véhicule i et le véhicule de destination K. En notant que quand le PDRe(t) = 0, les protocoles de BRR et GPSR sont identiques.

4.3 SCTP (Stream Control Transmission Protocol)

Parmi les protocole de streaming, on trouve le protocole UDP (User Datagram protocole)qui est non fiable avec aucune garantie sur la livraison,et aucun mécanisme de contrôle de congestion. Il y a donc une absence de notion du QoS en UDP, mais il est plus utilisé dans les transmissions des flux des données comme les vidéos.
SCTP est un autre protocole de couche transport qui prévoit le transfert fiable des données avec un mécanisme de contrôle de congestion. Il a été standardisé en 2000 et amélioré en 2007 dans le RFC 4960 [16]. Donc SCTP combine les traits d'UDP et de TCP et ajoute un peu de nouvelle fonctionnalité de son propre comme multi connexion (en anglais Multi homing), qui consiste, à être connecté à plusieurs fournisseurs d'accès à Internet afin d'améliorer la fiabilité de la connexion à Internet.
SCTP s'appuie également sur la fonctionnalité Multi-streaming dans lequel, les données peuvent être divisées sur des Multi connexions où en Multi-streaming ce qui permettent d'optimiser l'utilisation de la bande passante. Ces caractéristiques et d'autres qui seront expliquées ultérieurement peuvent être utilisées dans la transmission des multimédia (vidéo...).

4.3.1 Le fonctionnement du SCTP

SCTP est un protocole fiable de couche transport qui offre une distribution ordonnée de données sans erreur. Un certain nombre de fonctionnalités et des services sont offerts par SCTP qui sont discutés dans cette section.

Format des paquets de SCTP

SCTP utilise le même concept de port que TCP et UDP. Pour la détection d'erreurs de transmission, chaque paquet de SCTP est protégé par une somme de contrôle (checksum) de 32 bits (32-bit CRC checksum), qui est plus robuste que le checksum à 16 bits de TCP et UDP.
Le paquet SCTP est composé d'un en-tête commune et des modules spécifiques appelés chunks [23].

L'en-tête Commune

Chaque paquet SCTP contient un en-tête commun qui a 4 champs différents.
L'en-tête comporte 12 octets. Pour l'identification d'une association, il contient

également une valeur à 32 bits appelée balise de vérification (en anglais verification tag). La balise de vérification est utilisée pour se prémunir contre l'insertion des anciens messages erronés (cf.FIGURE 3.3).

Chunks

- Le paquet SCTP est formé de plusieurs morceaux (chunk), la fonction de Chunk Bundling gère l'assemblage du paquet SCTP et son réassemblage en réception.
- Les chunks sont divisés en deux classes : chunk de contrôle et chunk de données.
- Un chunk de contrôle est par définition un chunk qui contient des informations propres au contrôle et au maintien de l'association SCTP.
- Les chunks de données sont utilisés pour transporter des messages des utilisateurs à travers l'association.

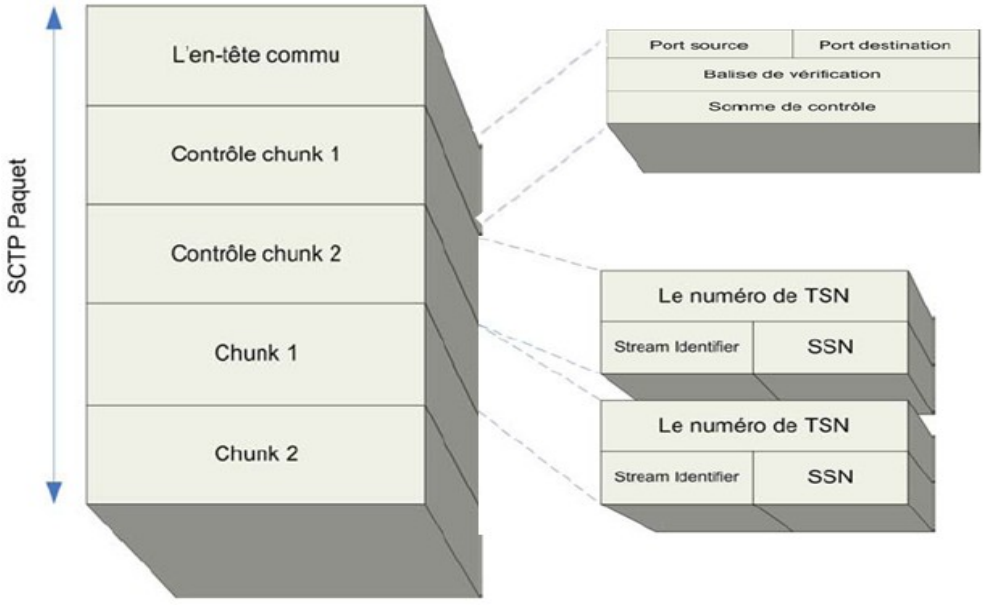

FIGURE 4.3 – le format d'un paquet SCTP [17]

- **Transmission Sequence Number (TSN) :** est renvoyé dans un chunk de contrôle pour chaque chunk de données reçu ; le récepteur utilise TSN pour la détection de perte et la duplication de données.
- **Identifiant de stream (SI : Stream Identifier) :** identifie les flux des chunks de données,ceci est utilisé lorsque SCTP transporte plusieurs flux dans une association (multistreaming).

- **Numéro de séquence de Stream (SSN : Stream Sequence Number) :** numéro de séquence pour chaque stream, ces numéros sont utilisés par le récepteur pour déterminer l'ordre de livraison.
- **U, vient de ((U)nordered) :** si cette valeur égale 1, alors ceci est un chunk de données non ordonné. Il n'y a pas de numéro de séquence de Stream pour cette donnée.
- **B, vient de ((B)eginning fragment) :** indique le premier fragment d'un message utilisateur.
- **E, vient de ((E)nding fragment) :** indique le dernier fragment d'un message utilisateur.
- **Payload Protocol Identifier :** précise un identifiant de l'application. Cet identificateur n'est pas utilisé par SCTP mais peut être utilisé par certains réseaux. Si cette valeur égale 0, alors aucun identifiant d'application n'est spécifié par la couche supérieure pour ces données.

L'établissement d'une association

Dans SCTP, une connexion est connue en tant qu'association. L'établissement d'une association (cf.FIGURE 3.4) est effectué après échange de quatre messages (et non pas trois comme avec TCP).pour offrir une meilleure protection contre les dénis de service.

L'opération d'établissement de connexion est faite par des étapes (cf.FIGURE 3.3) :

1. L'émetteur envoie un message INIT au récepteur pour initialiser une association.
2. A la réception du message INIT, le récepteur envoie une réponse INIT-ACK à l'émetteur. Ce message INIT-ACK contient les informations de configuration qui constituent un COOKIE.
3. A la réception de ce message INIT-ACK, l'émetteur envoie une réponse COOKIEECHO.
4. Le récepteur analyse les informations contenues dans le paquet COOKIE-ECHO reçu. Il vérifie ensuite la validité de la clé afin de s'assurer qu'il est bien l'émetteur d'origine de ce message de COOKIE. Si la clé est valide, le récepteur renvoie un message de COOKIE-ACK à l'émetteur et considère l'association comme établie.

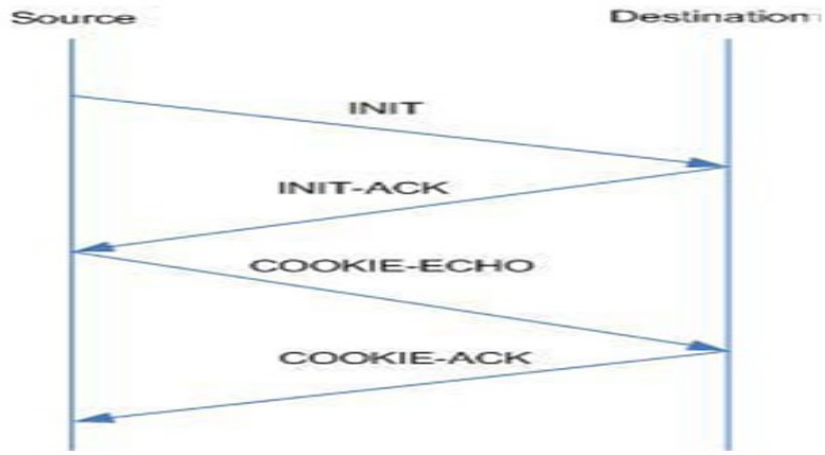

FIGURE 4.4 – établissement de connexion dans SCTP

Fermeture d'une association

Lorsque SCTP stoppe l'acceptation des données, il initie, à la demande de l'application, la fermeture de l'association.
La fermeture de SCTP utilise une procédure en trois messages :

1. L'émetteur envoie un message SHUTDOWN au récepteur, qui indique que le client est prêt à fermer la connexion.
2. Le récepteur répond en envoyant un message de SHUTDOWN-ACK.
3. L'émetteur envoie alors un message de SHUTDOWN-COMPLETE en retour au récepteur. Après cette procédure de fermeture, les deux extrémités ferment la communication (cf.FIGURE 3.5).

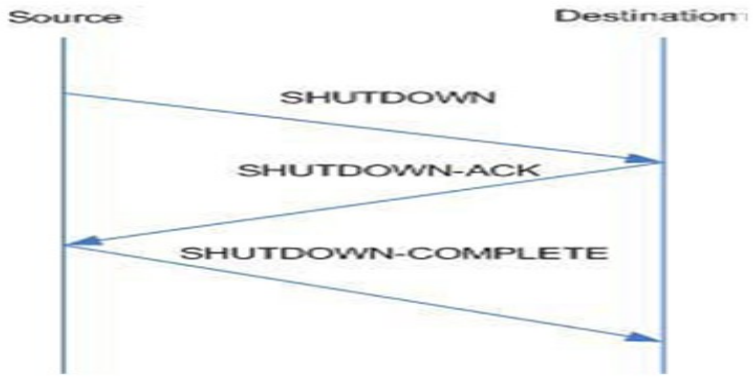

FIGURE 4.5 – La fermeture d'une connexion dans SCTP

4.3.2 Les caractéristiques du SCTP

La fiabilité de SCTP

SCTP offre un service de transmission fiable comme TCP. SCTP s'assure que les données sont transmises sur le réseau dans l'ordre et sans erreur. La transmission fiable de SCTP est également réalisée en détectant lorsque les données sont corrompues, dupliquées ou jetées [16]. Cette fonctionnalité transmet également les données endommagées si nécessaire.

Distribution ordonnée de données

La livraison des données non ordonnées est autorisée dans SCTP [23], comme illustré à la Figure suivante.
Dans le cas où un flux est affecté alors seulement le flux concerné est bloqué temporairement pendant que les autres flux seront autorisés à passer.
SCTP n'attend pas pour les messages à être ordonnés numériquement, en fait, il les traite à leur arrivée. Ces messages sont transférés de façon fiable par SCTP. Cette fonctionnalité de SCTP réduit au minimum les entêtes du message de réorganisation sur le serveur (cf.FIGURE 3.6).
Les informations nécessaires pour la livraison ordonnées des flux sont :

- U, vient de ((U)nordered)
- et (SSN : Stream Sequence Number)

Ces champs sont expliqués après cette section (cf.FIGURE 3.3)

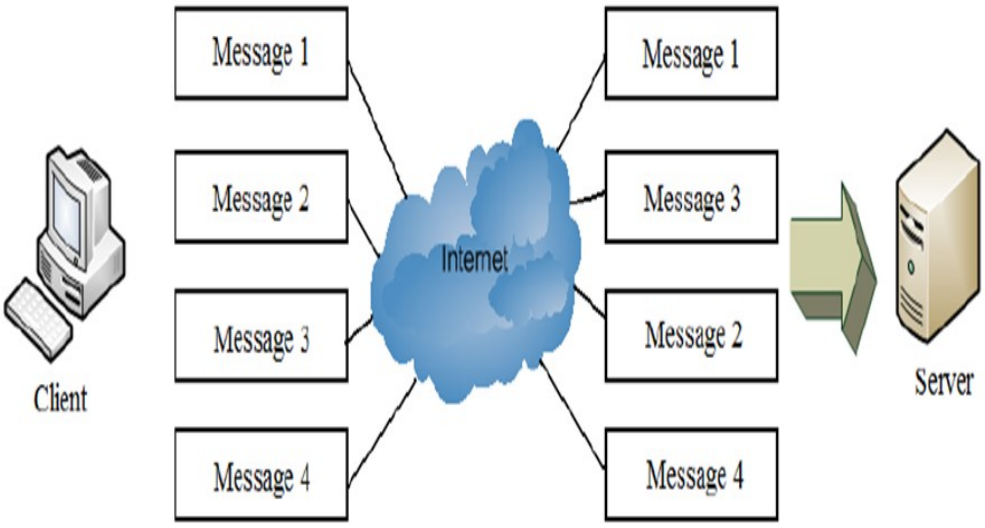

FIGURE 4.6 – La distribution de données dans SCTP

Multi-Streaming

TCP ne fournit pas un service de livraison un-à-plusieurs, il offre uniquement une livraison un-à-un.
SCTP permet d'envoyer plusieurs flux de données dans une connexion (ou plus précisément nommé association dans la terminologie SCTP).
Tous les flux dans une association sont liés à cette connexion spécifique, mais dans la transmission elles sont indépendantes. Un numéro de flux est donné à chaque flux, qui est codée dans les paquets.
Dans (cf. FIGURE 3.7), s'il y a une perte de paquets dans un flux (Comme exemple le flux 0) alors seulement ce flux spécifique (flux 0) sera bloqué (jusqu'à ce que les paquets perdus seront retransmises) sans affecter les autres flux (les flux de 1 à N) de l'association. Ce problème est connu comme le blocage de tête de ligne (en anglais head-of-line blocking) [16].

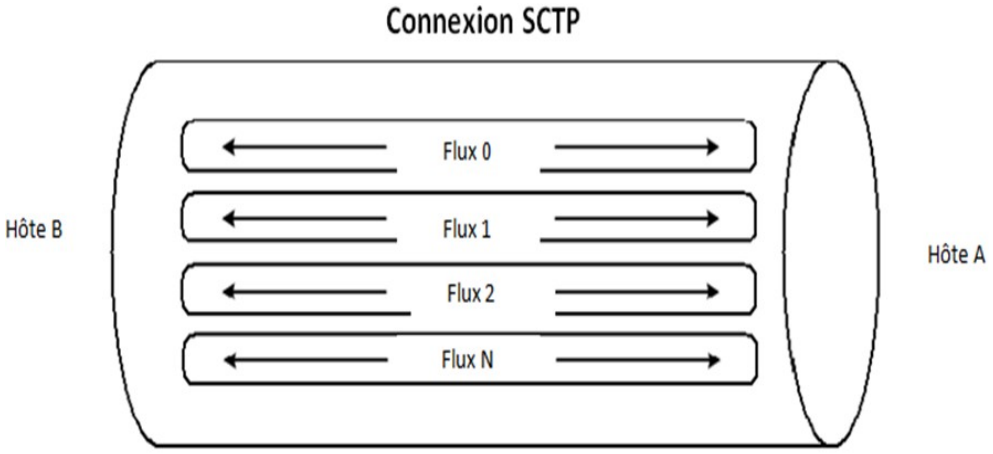

FIGURE 4.7 – Le multi-striming dans une connexiondu du SCTP

Multi- Connexion dans SCTP

La Multi connexion (en anglais Multi Homing) est la possibilité pour un protocole Internet d'utiliser plusieurs identifiants pour la même transmission des données [16]. Il est l'une des fonctions principales de SCTP.
Les principales applications du multi homing sont :

1. L'accélération des changements de réseau par l'obtention anticipée d'adresse.
2. Le partage de charge par une répartition du flux sur plusieurs chemins.
3. L'augmentation de la robustesse du réseau, par un basculement du flux d'information d'un chemin en panne vers un chemin en fonctionnement.

Dans la fonctionnalité multi-homing de SCTP, une interface est sélectionnée comme étant l'interface principale, tandis que l'autre devient secondaire, (cf.FIGURE 3.8) La communication commence à travers l'interface principale, mais dans le cas où l'interface principale devient inactive, la communication est basculée vers l'interface secondaire.
Lorsque l'interface principale est disponible à nouveau, la communication est assurée par l'interface principale.
Le mécanisme nommé heartbeat acknowledgment est utilisé pour vérifier et surveiller les interfaces primaires et secondaires. Ce mécanisme indique que l'interface est lente ou rapide. Si l'interface principale est plus lente par rapport à l'interface secondaire alors la communication est dirigée vers l'interface secondaire.

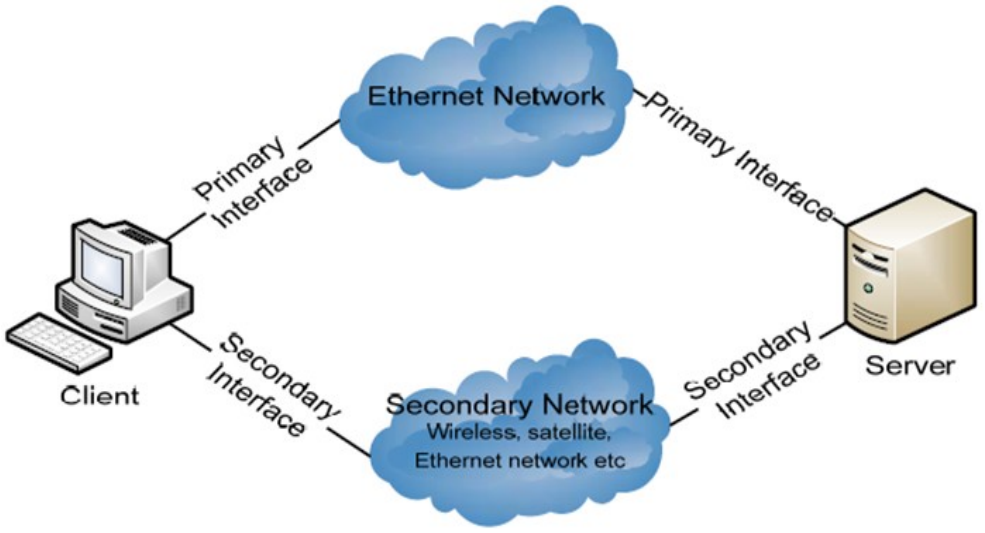

FIGURE 4.8 – Le multi-homing dans SCTP

4.4 Simulation

Les chercheurs dans la communauté scientifique recourent à l'utilisation des simulateurs de réseaux à cause de la difficulté de la mise en place des tests réels, surtout de grande ampleur, c'est-à-dire mettant en œuvre plus d'une dizaine de terminaux. La première difficulté est de réunir un grand nombre de nœuds (de l'ordre d'une centaine). Il faut pour cela obtenir des moyens financiers très important .
De plus, si l'objectif de réunir une centaine d'entités mobiles était atteint, il resterait encore à rassembler un panel de " testeurs " équipés d'une station d'expérimentation. Il est aussi nécessaire d'équiper les utilisateurs d'un système permettant de tracer leurs déplacements pour exploiter les données relatives à l'application étudiée, en fonction de leurs comportements au sein du champ d'opération [24].
La simulation permet aussi de reproduire une expérience dans des conditions identiques que le réel afin d'extraire des statistiques. Par exemple, on peut maîtriser et reproduire certains paramètres du comportement des utilisateurs simulés, comme leur vitesse de déplacement.
L'utilisation d'un simulateur est inévitable si on considère le besoin de collecter des informations globales. En effet, lors de tests réels sur des réseaux comme VANets on ne peut pas facilement obtenir d'information globale sur le comportement d'une application. comme essais en simulation en revanche le permettent.

Pour rassembler les détails qui sont nécessaires pour la simulation, il existe de nombreux simulateurs. Certains d'entre eux sont sous licence commerciale et certains d'entre eux sont gratuits. Les divers simulateurs réseaux commerciaux comme OPNet,QualNet,OMNET++, etc...[25], sont des simulateurs de trafic commerciaux puissant visant à rassembler les éléments requis en supportant GUI (Graphique User Interface). L'acquisition d'une licence unique pour ces logiciels commerciaux coûte très chère.
Le simulateur utilisé dans ce mémoire appartient au deuxième type.

4.4.1 Le simulateur NS-2

NS-2 est le plus connu et le plus utilisé des simulateurs de réseaux dans les recherches académiques sur ce domaine. La majorité des protocoles de réseaux ont été implémentés sous ce simulateur [5] car il est open source et gratuit .
Il est développé à l'ISI (Information Sciences Institute) en Californie (Marina del Rey). NS-2 est basé sur l'utilisation d'événements discrets et a été développé en premier lieu pour simuler des réseaux filaires. Les supports de

WiFi et de Bluetooth n'ont été introduits que plus tard [24].

NS-2 utilise deux langages, C++ et OTCL. La raison pour cette utilisation est que les différentes langages ont des exigences différentes : par exemple simulation de protocoles nécessite une manipulation efficace des octets et des en-têtes de paquets. En revanche, dans les études de réseau où le but est de modifier certains paramètres et d'examiner rapidement un certain nombre de scénarios, le temps de changement du modèle et d'exécution est plus important.
Dans ns2, le langage de programmation C++ est utilisé pour la mise en œuvre détaillé d'un protocole et en général pour les cas où tous les paquets d'un flux sont à traiter(par exemple, pour mettre en place un nouveau protocole de routage), d'autre part, Otcl est adapté pour l'installation et la configuration. Otcl s'exécute très lentement, mais il peut être modifié très rapidement, ce qui facilite la construction des simulations.
Dans ns2, les objets C++ compilés peuvent être accessibles à l'interprète d'Otcl, de cette façon, les objets C++ peuvent être contrôlés au niveau OTcl.

4.4.2 Le modèle de mobilité

L'évolution de la connectivité entre les nœuds du réseau est la caractéristique qui différencie le plus un réseau mobile d'un réseau statique. Cette évolution est généralement liée aux déplacements physiques des stations. Ils doivent donc être pris en compte pour que l'algorithme simulé évolue dans des conditions similaires à ce que l'on pourrait observer dans un contexte réel. Pour cela, il existe différents modèles de mobilité qui définissent les changements des positions des nœuds du réseau. Ces modèles ont pour objectif de régir les déplacements des stations et de permettre de recréer les mêmes conditions expérimentales plusieurs fois.

Une équipe de recherche de l'université USC (Université of SouthernCalifornia) a proposé un générateur de mobilité pour les VANet appelé IMPORTANT. C'était dans le cadre du projet MARMALADeS (Multicast and Resource Management for Large-Scale Ad-hoc and Sensor Networks), Son code source est téléchargeable depuis le site web du projet. Ce générateur est capable de générer beaucoup de modèles pour les VANet comme les modèles Freeway et Manhattan.

Le modèle de mobilité utilisé dans notre simulation est le modèle FREEWAY, ce modèle peut être utilisé dans l'échange de l'état du trafic ou suivi d'un véhicule sur une autoroute. Il est proposé pour simuler le comportement de mouvement des nœuds mobiles sur une autoroute [26].

Ce modèle est caractérisé par :

1. Chaque nœud mobile se limite à sa voie de circulation sur l'autoroute.
2. La vitesse du nœud mobile est temporellement dépendante à sa vitesse précédente.

Les fichiers de trace générés sont compatibles avec le format requis par ns-2. Donc que l'utilisateur peut injecter directement les fichiers de trace générés par ce générateur dans le simulateur ns-2 et exécuter les simulations.

4.4.3 Visualisation des résultats

Afin d'être capable de calculer les résultats de la simulation, les données doivent être collectées d'une certaine façon. Ns2 prend en charge deux méthodes principales : les traces et les moniteurs.
Les fichiers traces peuvent sauvegarder les traces des paquets liés à chaque événement tel que la perte de paquet ou l'arrivée à une file d'attente ou un lien. le nombre d'arrivée des paquets.

Les moniteurs offrent un moyen de collecter les quantités, telles que le nombre de perte des paquets ou le nombre des paquets arrivés dans la file d'attente. Le moniteur peut être utilisé pour collecter ces quantités pour tous les paquets ou juste pour un flux spécifié.

4.4.4 Le type de trafic

Le CBR (Constant Bit Rate) est un type de trafic qui génère les paquets avec un débit binaire constant l'objet CBR est dérivé de la classe d'OTcl Application/Traffic/CBR, les paramètres les plus utilisés qui caractérisent l'objet CBR sont : rate_ : le taux d'envoi. interval_(Optionnel) : l'intervalle entre les paquets.
packetSize_ : la taille constant des size paquets générées .
maxpkts_ :le nombre maximum des parquets a envoyées (par default 228).

Les métriques d'evaluation de performances :

Les mesures de la performance utilisées dans ce mémoire sont les suivantes : **Le taux de perte de paquets**
c'est le nombre total de paquets perdus pendant la transmission sur le nombre total des paquets envoyés. Où le petit taux signifie plus de performance du protocole.
La perte des paquets est calculée en prenant la différence entre le nombre total de paquets transmis et reçus.

Taux de perte des paquets = nombre de paquets perdus / nombre total des paquets envoyés.
Où Nombre de paquets perdus = nombre total de paquets transmis - nombre total des paquets reçus.
Débit.
Débit est la quantité de données qu'un véhicule reçoit de l'expéditeur dans un intervalle de temps spécifique.
Débit = total des données reçues/la durée total.
La durée totale est la différence entre les moments de réception du dernier paquet et premier paquet émis.
Délai .
Délai de bout en bout est le temps total pris par un paquet au cours de la transmission dans un réseau d'une entité de communiquer à l'autre. Le délai est calculé en prenant la différence entre les moments de l'envoi et la réception d'un paquet.
Délai = temps d'arrivée du paquet (A) - temps d'envoi du paquet (A).
Taux de livraison des paquets (PDR) : la quantité de données qu'un véhicule a envoyé dans un intervalle de temps spécifique.
BDR =le total des données envoyé / temps total .

4.4.5 Les protocoles choisis

Les protocoles qu'on a choisit dans notre simulation sont TCP et SCTP. On choisit TCP parce qu'on le considère comme une référence pour faire la comparaison.
Et on a choisit le SCTP pour plusieurs raisons :

- Les différences principales avec TCP sont le multi-homing et le concept de flux (Stream) à l'intérieur d'une même connexion, (ces deux concepts sont déja expliqués dans ce chapitre) Alors que dans TCP un flux fait référence à une séquence d'octets, un flux SCTP fait référence à une séquence de messages (courts ou longs).
- De plus, des fonctionnalités qui sont optionnelles dans TCP ont été incluses dans la spécification de base de SCTP, telles que le Selective Acknowledgment, permettant d'annoncer la réception de datagrammes erronés ou dupliqués ou encore le support de Explicit Congestion Notification (ECN).
- afin d'augmenter la sécurité dans les VANets, les attaques simples de synchronisation (de type SYN attack) qui affectent TCP ne sont plus possibles avec SCTP. Ce nouveau protocole inclut aussi des mécanismes protégeant les applications contre le Head of Line Blocking.

Les paramètres de simulation

Dans nos simulations, pour évaluer les performances des protocoles de la couche transport spécifiés auparavant, nous avons choisi les paramètres suivants :

Type de trafic	CBR
Taille du paquet	500 octets
La durée de simulation	25 secondes
Longueur de la route (m)	2000
La vitesse maximale	100 km/h
La vitesse minimale	50 km/h
Le nombre des nœuds	Variables entre 20 et 100
Le protocole de routage	GPSR
Les protocoles de transport	TCP et SCTP
Le modèles de mobilité	FREEWAY

TABLE 4.1 – Les paramètres généraux de simulation

Les résultats de simulation

Dans ce travail, on a comparé les performances des protocoles de la couche transport (TCP, SCTP), où le flux de données généré est de débit constant (CBR), avec un taille de paquet de 500 octets, chaque simulation a durée 25 secondes,

L'environnement utilisé est l'environnement de FREEWAY comme illustrées dans le tableau TABLE 3.1.
Les graphes ci-dessous va présenter la performance des protocoles TCP et SCTP individuellement dans VANets. Les graphes sont obtenus en basant sur les paramètres suivants :

1. Débit
2. Le taux de perte des paquets.
3. Le taux de livraison des paquets (PDR).
4. le délai moyen de bout en bout : en calculant le moyen des délais.

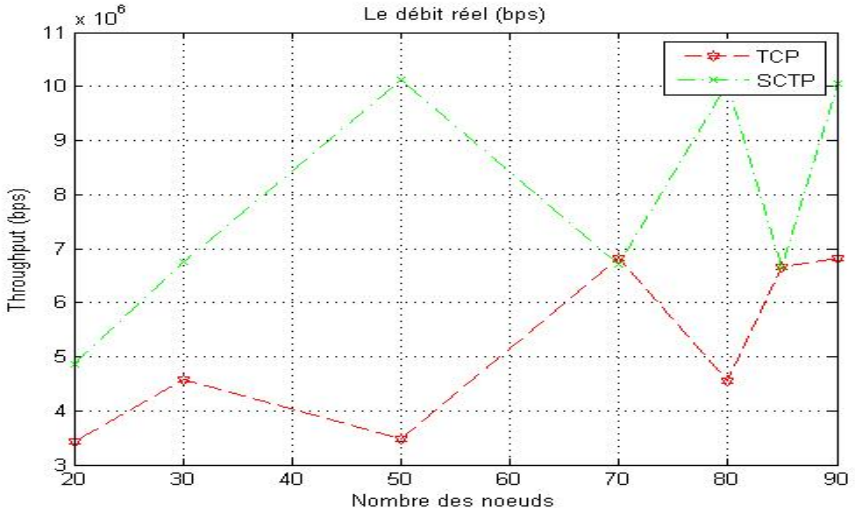

FIGURE 4.9 – graphe de débit pour TCP et SCTP dans les VANets

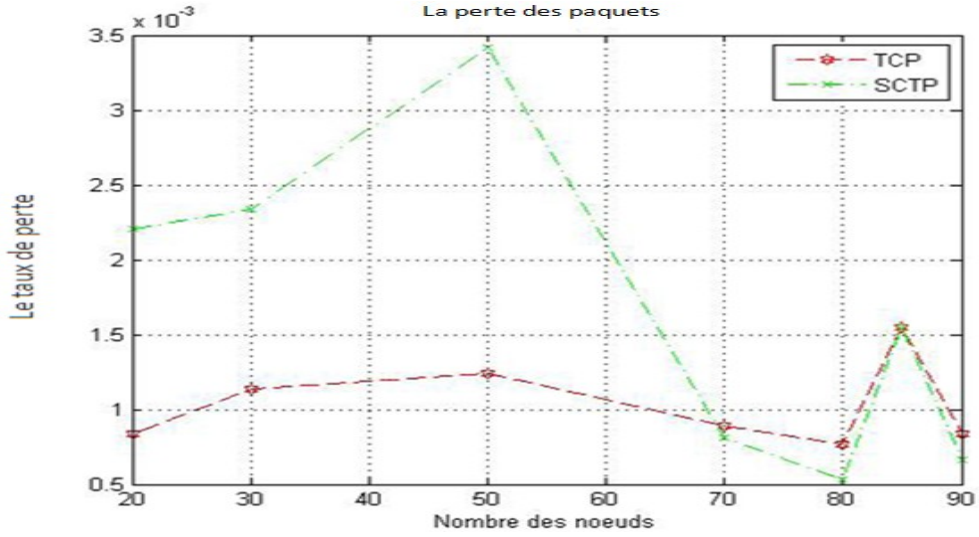

FIGURE 4.10 – graphe de taux de perte pour TCP et SCTP dans les VANets

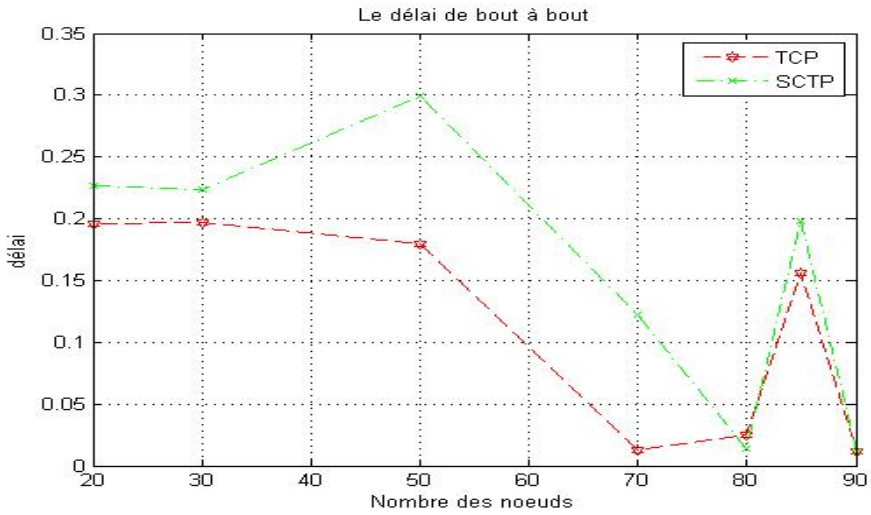

FIGURE 4.11 – graphe de délai pour TCP et SCTP dans les VANets

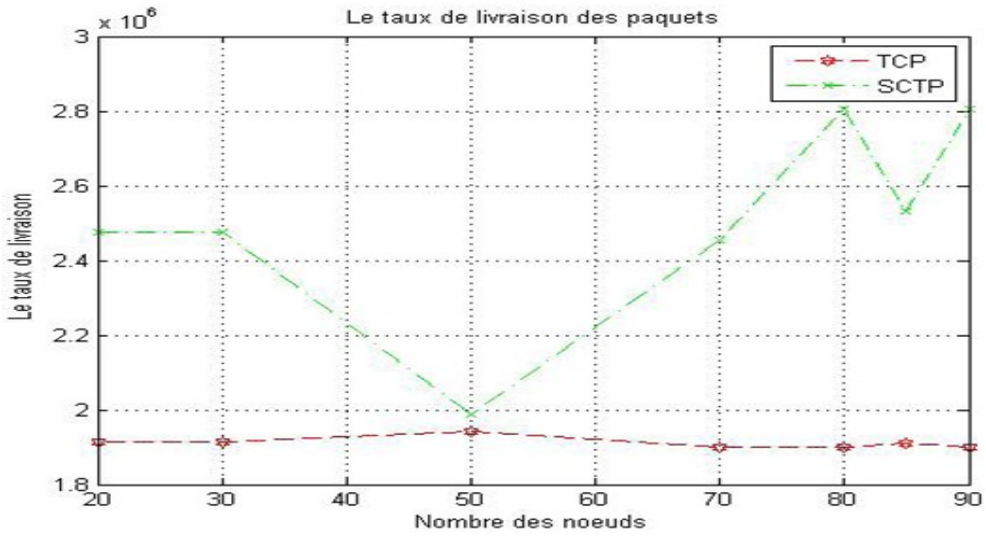

FIGURE 4.12 – graphe de taux de livraison des paquets pour TCP et SCTP dans les VANets

4.4.6 Discussion

La FIGURE 3.9 montre que le débit du SCTP est plus élevée par rapport au TCP quelque soit le nombre des véhicules dans la route.
Alors le SCTP est meilleur que TCP avec cette mesure. Cela revient au mécanisme utilisé par SCTP qui est le multi-streaming, qui permet au SCTP de pouvoir continuité d'envoi des flux, même en cas de perte d'un segment du flux.
La perte d'un segment comme vu auparavant n'a pas une aucune conséquence sur les autres flux. Par contre, TCP doit attendre jusque à la retransmission du segment perdu.
Le débit du SCTP est performant malgré que le taux de perte du SCTP est grand par rapport au TCP, ce qui confirme la performance de la technique de multi-streaming (cf.FIGURE 3.10).
Dans la FIGURE 3.12, le PDR du protocole SCTP est grand que celle dans TCP, chose qui est évidente en basant sur les deux figures précédentes. Ce PDR permettra d'augmenter la fiabilité des protocoles de couche transport.
Mais pour le délai de transmission,(cf.FIGURE 3.11),on remarque que SCTP donne la même performance que TCP en cas de forte densité, car les paquets dans SCTP entre en collision , ce qui influe sur le délai moyen global.
A cause du délai élevé dans certain cas, on peut conclure qu'on doit adapter SCTP en minimisant le délai pour appliquer au environnement véhiculaire, pour cela on propose d'adapter GPSR pour choisir le nœud forwarder comme il est expliqué dans le fin de section 1 de ce chapitre, et que SCTP n'est pas très applicable dans les environnements véhiculaires.

4.5 Conclusion

Dans ce chapitre, on a présenté par une description détaillée du protocole du basé sur TCP nommé VANet TCP adapté au VANet,par solution de problème de perte dans les réseaux a forte mobilité.

Le deuxième c'est le protocole SCTP qui est un protocole qui supporte le streaming, il combine entre les protocoles TCP et UDP.

Et enfin, on a essayé par une simulation dans les réseaux véhiculaire d'analyser les performances du SCTP faisant la comparaison avec le protocole TCP standard .

Chapitre 5

Conclusion générale

Les réseaux ad hoc véhiculaires, présentent une application récente des réseaux mobiles qui a favorisé une formidable évolution du système de transports, dans l'objectif d'augmenter la sécurité et d'accroitre le confort.
Le développement de protocoles pour ce type de réseaux qu'ont des caractéristiques particulières, s'avère une tâche indispensable pour la mise en œuvre de ces applications.
Le but principal de ce mémoire était de mieux comprendre le fonctionnement des protocoles fiables de la couche transport, et en particulier le protocole TCP, et d'étudier les mécanismes pour son adaptation aux environnements véhiculaires.
Pour cela, on a présenté tout d'abord les réseaux VANet avec leurs caractéristiques dans le premier chapitre. Ensuite dans le deuxième chapitre, on a détaillé les différents protocoles existant dans les réseaux filaires, sans- fil ou Ad hoc classiques.
Dans le chapitre trois, on a essayé de présenter deux protocoles de transport appelés VANet TCP et SCTP, avant d'analyser les performances de TCP en les comparant avec SCTP en variant à chaque fois les paramètres influant (le nombre et la vitesse des nœuds).
Les résultats ont montré que, en plus du support de transmission, la mobilité est l'handicap principal pour appliquer TCP directement dans ces réseaux.
Comme travaux futurs, on suggère de proposer un protocole "cross-layer" qui adapte la couche réseau au besoin de la couche transport en modifiant les mécanismes et les métriques du choix des nœuds.

Acronymes

TCP	Transport Control Protocol
IVC	communications inter-véhicules
ITS	intelligents transport systèmes
MANET	Mobile Ad hoc Network
VANet	Vehicular Ad hoc Network
WPAN	Wireless Personal Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WWAN	Wireless Wide Area Network
IBSS	Indépendant basic service set
RSU	Road Side Unit
V2I	Véhicule à Infrastructure
I2V	Infrastructure à Véhicule
DSRC	dedicated short range communications
WAVE	wireless access in vehicular environnement
IEEE	Institute of Electrical and Electronic Engineer
MAC	Medium Access Control
DSDV	(Destination Sequence Distance Vector)
OSLR	Optimized Link State Routing Protocol
DSR	Dynamic Source Routing
AODV	Ad-hoc On demand Distance Vector
GPSR	Greedy Perimeter Stateless Routing for Wireless Networks
WEP	Wired Equivalent Privacy
ACK	Abrév de ACKnowledged
ECN	Explicit Congestion Notification
GUI	graphical User Interface

Bibliographie

[1] Sofiane Khalfallah, Moez Jerbi, Mohamed Oussama Cherif, Sidi Mohammed Senouci, and Bertrand Ducourthial. Manuscrit expérimentations des communications inter-véhicules. *publié dans Colloque Francophone sur l'Ingénierie des Protocoles (CFIP)*, 2008.

[2] B. Jarupan and E. Ekici. Article : A survey of cross-layer design for vanets. *Ad Hoc Networks "elsevier"*, 2011. The Ohio State University, Columbus ,USA.

[3] GUY PAJOLLE. Les réseaux 5ème édition, 2006.

[4] Nouha BACCOUR SELLAMI. Master's thesis : conception d'une nouvelle stratégie de routage dynamique pour les réseaux mobiles ad hoc. *Université de Sfax*, page 91, 2006.

[5] Noureddine CHAIB. Mémoire de magister : La sécurité des communications dans les réseaux vanet. *UNIVERSITE ELHADJ LAKHDER - BATNA*, page 113, 2011.

[6] Amadou Adama Ba. Maters's thesis : Protocole de routage basé sur des passerelles mobiles pour un accès internet dans les réseaux véhiculaires. *Université de Montréal*, 2011.

[7] Vaishali D. Khairnar and S.N. Pradhan. Article : V2v communication survey - (wireless technology). *IJCTA*, 2010. ISSN :2229-6093.

[8] Oscar Trullols Cruces. Masters's thesis : Applying delay tolerant protocols to vanets. *Univ. of Catalonia*, 2008.

[9] Zaydoun Yahya Rawashdeh and Syed Masud Mahmud. chapitre book :communications in vehicular networks. *University of Detroit, Michigan,USA*.

[10] Gongjun Yan, Nathalie Mitton, and Xu Li. manuscript publie : Reliable routing in vehicular ad hoc networks. *"The 7th International Workshop on Wireless Ad hoc and Sensor Networking (WWASN 2010),Italy"*, 2010.

[11] Saadaoui Meriem. Mémoire master : Correction des erreurs gps dans les réseaux vanets par fusion de données. *université Ammar Telidji Laghouat*, 2011.

[12] Bruno Péan. support de cours résaux. *eisti,URL="http ://bp.perso.eisti.fr/doc/reseaux/"*, 2010.

[13] Yuvaraju B. N and Niranjan N Chiplunkar. Article : Scenario based performance analysis of variants of tcp using ns2-simulator. *International JOURNAL of Advancements in Technology IJoAT*, October), notes=ISSN 0976-4860 2010.

[14] Pasi Sarolahti. Master's thesis : performance analysis of tcp enhancements for congested reliable wireless links. 2000.

[15] Aiyathurai Jayananthan. *PHD Thesis : TCP PERFORMANCE ENHANCEMENT OVER WIRELESS NETWORKS*. PhD thesis, University of Canterbury New Zealand, 2007.

[16] Sakuna CHAROENPANYASAK. Masters's thesis : Optimisation intercouches du protocole sctp en réseaux ad hoc. *Université de Toulouse*, 2008.

[17] Muhammad Ijaz. Masters s thesis :trasmission control protocol (tcp) performance evaluation in manet. *BLEKINGE INSTITUTE OF TECHNOLOGY*, 2009.

[18] Marc Bechler, Sven Jaap, and Lars Wolf. An optimized tcp for internet access of vehicular ad hoc networks. *IFIP International Federation for Information Processing*, 2005.

[19] TCP in Wireless Mobile Networks. `"www.cs.sunysb.edu/\~jgao/CSE370-spring06/lecture17.pdf"`,13 juin 2012, 2006.

[20] S. M. Mousavi, H. R. Rabiee, M. Moshref, and A. Dabirmoghaddam. These de doctorat : Communications dans les réseaux fortement dynamiques. *Université Paris-Sud 11*, juin 2010.

[21] Jian Liu and Suresh Singh. Article : Atcp : Tcp for mobile ad hoc networks. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, JULY 2001.

[22] Wantanee Viriyasitavata, Fan Bai, and Ozan K. Tonguz. Toward end-to-end control in vanets. *IEEE Vehicular Networking Conference (VNC)*, Nov 2011.

[23] Aamir Hassan. Master's thesis : Vanet simulation. may 2009.

[24] Lionel Barrère. these doctorat : Etude et proposition de services dans les réseaux mobiles militaires de type manet. 2009.

[25] Ranjitha Shivarudraiah. Maters's thesis : Stcp : A new transport protocol for high speed networks. *Université Georgia State*, Decembre 2009.

[26] S. M. Mousavi, H. R. Rabiee, M. Moshref, and A. Dabirmoghaddam. Article : Mobisim : A framework for simulation of mobility models in mobile ad-hoc networks. *Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2007.