Synthèse sur les principaux protocoles MAC proposés pour les VANETs

Bennai Yani Athmane, Pr.Louiza Bouallouche-Medjkoune, Dr.Samira Yessad

Doctoriales de Recherche Opérationnelle, le 12 et 13 Décembre 2018

Résumé

A cause de la nature particulière des réseaux véhiculaires par rapport aux réseaux adhoc classiques (grande mobilité des nœuds, topologie dynamique du réseau…etc), le processus de conception de protocoles d'accès au canal (MAC) offrant des performances satisfaisantes peut s'avérer difficile.Nous présentons, dans ce travail, une synthèse sur les principaux protocoles MAC proposés spécialement pour les VANETs dans la littérature, ainsi que des critiques et mises en lumière des limitations de ces derniers.

Introduction

La communication inter-véhicules devient une des priorités dans le domaine de la technologie automobile, et plusieurs fonctionnalités et applications sont étudiées et développées pour les ITS (Intelligent Transportation Systems). Dans un VANET (Vehicular AdHoc Network), on distingue deux types de nœuds : Les RSU (Road Side Units) qui sont des infrastructures installées sur le bord des routes et qui servent de source et de relais pour les informations circulant sur le réseau, et les OBU (On Board Units) qui sont des équipements intégrés aux véhicules pour le traitement de données et la gestion des communications. Ces communications peuvent se passer soit entre deux véhicules, ce qu'on appelle IVC (Inter Vehicular Communication), ou bien entre un véhicule et une infrastructure (VRC-Vehicule to Roadside Communication). Toutefois, la conception de protocoles efficaces pour les VANETs est rendue difficile par les caractéristiques particulières de ce type de réseaux par rapport aux réseaux AdHoc classiques, telle que la topologie dynamique ou encore la grande mobilité des nœuds. Cette difficulté s'applique donc aussi au développement de protocoles d'accès au canal (MAC) satisfaisants à cause des métriques de performances exigées sur cette couche. Les protocoles MAC dans les VANETs peuvent être classifiés en trois catégories selon la manière dont l'accès au canal est géré : à division de temps, tolérants aux collisions et les protocoles à antennes directionnelles. Dans ce travail, nous présentons une synthèse des principaux protocoles MAC proposés dans la littérature pour les VANETs, ainsi qu'une critique et précision sur les limitations de chacun.

I-MCTRP

Dans [1], Bi et al. ont proposé un protocole utilisant des anneaux et jetons sur plusieurs canaux de communication (multi-canal) appelé MCTRP (Multi Channel Token Ring Protocol). Le but de ce protocole était de concevoir une méthode MAC déterministe qui puisse gérer de manière autonome l'organisation des nœuds du réseau en anneaux afin de maximiser la bande passante et réduire le temps de latence. Pour la communication, chaque nœud est équipé de deux radios : La première est constamment connectée au canal 178 du « WAVE » et dédiée aux transmissions inter-anneaux, la deuxième radio est quand à elle connectée à un des six canaux « WAVE » restants et est dédiée aux communications au sein de chaque anneau quel que soit le type de message transmit (message de sécurité, de coordination ou de données).

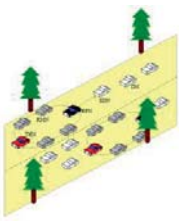

Figure I.1 : Vue d'ensemble de MCTRP

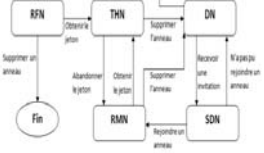

Figure I.2 : Changements d'états dans MCTRP.

Ce protocole montre certaines faiblesses qui sont notamment liées à sa fragilité. En effet, MCTRP est très dépendant des nœuds présents sur les anneaux, par exemple si un responsable d'anneau (Ring Leader) se déconnecte ou sort de la portée du réseau, toutes les entités dépendantes de cet anneau vont à leur tour se déconnecter, nous dirons donc que MCTRP est plus adapté à des réseaux avec une faible mobilité. De plus, le protocole se base sur une connectivité entre tous les nœuds d'un anneau (car le jeton doit circuler de manière séquentielle d'un nœud à l'autre), or nous savons que dans la pratique les réseaux véhiculaires sont très instables et leur topologie très imprévisible ce qui rend difficile l'implémentation de MCTRP dans des scénarios réels.

II-IEEE 802.11p

802.11p est une partie importante de la pile de protocoles « WAVE » (Wireless Access in Vehicular Environnements) proposée par l'IEEE. 802.11p utilise la distribution d'accès au canal avancée présente dans la méthode MAC « EDCA », qui est elle-même une amélioration de la fonction de coordination distribuée (DCF) qui figure dans 802.11. Cette méthode utilise CSMA/CA (qui évite les collisions), un nœud souhaitant transmettre sur le canal commence d'abord par lancer une écoute, il envoie ses données s'il trouve que celui-ci est libre, par contre si le canal est occupé le nœud devra effectuer une attente aléatoire avant de retenter une autre fois de transmettre.

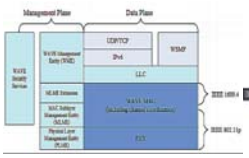

Figure II.1:Pile de protocoles WAVE.

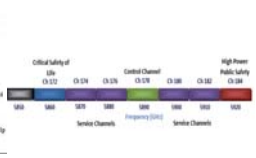

Figure II.2:Allocation des canaux dans WAVE

La méthode MAC de 802.11 se base sur l'utilisation d'acquittements (ACK), c'est-à-dire qu'un nœud ayant transmis vers son destinataire attends un ACK confirmant la réception des données, si aucun ACK n'est reçu après un laps de temps défini, une attente aléatoire est imposée à l'envoyeur avant de pouvoir retransmettre son message.

Bien que cette méthode constitue une base solide pour les futures avancées dans le domaine MAC au sein des VANETs de part sa simplicité, elle peut néanmoins être qualifiée de « fragile » et n'est surement pas optimale dans le cadre d'une implémentation massive dans des scénarios réels. En effet, dans [2] les résultats de la simulation montrent clairement une forte chute de performances dans le cas d'un système chargé, 802.11p devrait donc être configuré au sein de réseaux avec de petites tailles de paquets et une large période entre les messages périodiques. Pour finir CSMA est inapproprié pour le trafic de données en temps réels à cause de son caractère imprévisible, puisque aucune borne maximale n'est fixée pour les temps d'attente, les nœuds du réseau pourraient faire face à des délais trop importants et donc irréalisables.

III-DMMAC

Dans [3], Lu et al. ont proposé un nouveau protocole d'accès au canal pour les réseaux véhiculaires basé sur la pile WAVE appelé DMMAC. Ce protocole vise avant tout à garantir un accès sans collisions au médium pour la transmission de messages de sécurité sur l'intervalle de temps CCHI (chaque intervalle de synchronisation est divisée en deux parties : CCHI pour le canal de contrôle et SCHI pour les canaux de service). DDMAC utilise une combinaison entre TDMA et CSMA/CA.

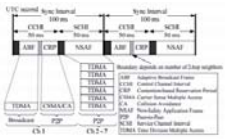

Figure III.1: Structure des messages dans DMMAC.

L'intervalle SCHI est dédié aux messages d'information, tandis que CCHI est consacré aux messages de sécurité. CCHI est divisé en deux sous-intervalles, ABF et CRP, qui sont séparés par une frontière flexible qui s'adapte au nombre de nœuds à portée. ABF est utilisé pour la diffusion (multipoint) de messages de sécurité (similaire au CCH dans WAVE), à la différence près que pour ABF des transmissions sans collisions peuvent être réalisées grâce à l'utilisation de TDMA. Les nœuds ont accès à des slots d'1ms chacun pour être alloués, une fois qu'un nœud a pu acquérir un slot il devra envoyer une trame d'information (IF) qui contient son identifiant (ID), des informations qui permettront à ses voisins de calculer la frontière entre ABF et CRP, ainsi que sa table d'allocation des slots (SAT). CRP est quand à lui utilisé pour prétendre à un slot et un canal de la part des nœuds pour la transmission de messages d'information. Les demandes durant l'intervalle CRP sont basées sur une authentification en trois étapes entre deux nœuds, une requête puis une réponse puis un acquittement. Les deux nœuds peuvent ainsi se mettre d'accord sur un slot et un canal pour commencer la transmission.

Dans leur travail, Lu et al. ont effectué leurs simulations dans un environnement très basique, avec un scénario impliquant une autoroute droite et une population ne dépassant pas les 30 véhicules, cela veut dire qu'il y avait très peu de risque que les slots soient saturés de part les paramètres de départ choisis. De plus, ce modèle ne prends pas en compte les différents événements pouvant survenir dans un scénario réel (changement de voie, dépassements. . .etc), les résultats de la simulation ne sont donc pas très représentatives du comportement de DMMAC dans des conditions réelles.

IV-STDMA

STDMA est une méthode MAC basée sur le très répandu TDMA dont le but est de garantir de bons délais de transmission pour ce qui est des messages de sécurité critiques et elle propose des communications présentant peu de risques de collisions. Un nombre défini de slots forment une trame et le temps GPS est utilisé afin de synchroniser les slots des nœuds du réseau, chaque nœud choisit ainsi un ensemble de slots auxquels il pourra accéder. La structure des messages du protocole est détaillée ci-dessous.

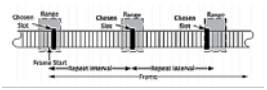

Figure IV.1: Structure des trames dans STDMA

La méthode suit ensuite le fonctionnement standard de TDMA une fois que les slots ont été affectés, chaque nœud transmet ses données ainsi qu'un message d'urgence (optionnel) durant le slot qui lui est affecté. STDMA présente toutefois des lacunes qui le rendent inadapté à certaines situations,comme on peut le voir dans [4], puisqu'il se base principalement sur l'allocation de temps, un slot est donc perdu a chaque fois qu'un nœud n'a pas besoin de transmettre (et qu'un slot lui a été affecté). De plus, ce protocole à été conçu pour gérer une faible charge de données pour par exemple annoncer des informations de positionnement uniquement, il n'est donc pas approprié lorsqu'on à affaire a des grandes quantités de data.

V-VeMAC

Dans [5], Hassan Aboubakr Omar et al. ont présenté un protocole MAC multicanaux déterministe nommé VeMAC visant à garantir des liaisons point à point et multipoint efficaces, avec un faible taux de collisions. Chaque nœud est équipé de deux récepteurs radio, le premier est constamment connecté au canal de contrôle (c0), tandis que le second peut être connecté a chacun des m canaux de service (c1..cm) et la synchronisation se base sur le signal GPS. Les paquets transmis sur le canal de contrôle sont constitués de quatre champs : L'en-tête, l'annonce de service (AnS), l'acceptation de service (AcS) et le champ High Priority Short Applications. Lors de sa transmission sur c0, chaque message doit inclure dans son en-tête les slots réservés par tous ses voisins à un saut afin d'éviter le problème du terminal caché (Hidden Termial), cela permet au récepteur de connaitre tous les slots de temps utilisés par les voisins et ainsi déterminer quels sont ceux qu'il pourra réserver (ceux qui sont libres). La désignation de slots sur les canaux de service sont effectués par le fournisseur, on appelle fournisseur tout nœud offrant un service sur un canal de service donné dans le champ AnS sur c0, et un utilisateur tout véhicule ayant reçu cette offre et décidé de s'en servir (utiliser le service), c'est donc la responsabilité du fournisseur d'allouer les slots à tous les utilisateurs.

Header	AnS	AcS	High Priority Short Applications

Figure V.1:Format des paquets transmis sur le canal de contrôle.

VeMAC utilise les sept canaux alloués pour le DSRC (un canal de contrôle et six canaux de service), et réduit de manière effective le taux de collisions. Il présente néanmoins quelques manquements, par exemple la taille importante des paquets de contrôle circulant sur c0 peut conduire à un excès (Overhead) et ainsi à des retards. De plus, VeMAC manque de souplesse en ce qui concerne certains scénarios, la taille fixe des slots n'est pas adaptée à des situations où le nombre de véhicules de chaque coté de la route varie (par exemple dans le cas des autoroutes).

[1] Bi, Y., Liu, K. H., Cai, L. X., Shen, X., & Zhao, H. (2009). A multi-channel token ring protocol for QoS provisioning in inter-vehicle communications. *IEEE Transactions on Wireless Communications*, *8*(11).

[2] Bilstrup, K., Uhlemann, E., Strom, E. G., & Bilstrup, U. (2008, September). Evaluation of the IEEE 802.11 p MAC method for vehicle-to-vehicle communication. In *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th* (pp. 1-5). IEEE.

[3] Lu, N., Ji, Y., Liu, F., & Wang, X. (2010, April). A dedicated multi-channel MAC protocol design for VANET with adaptive broadcasting. In *Wireless Communications and Networking Conference (WCNC), 2010 IEEE* (pp. 1-6). IEEE.

[4] Bilstrup, K., Uhlemann, E., Ström, E. G., & Bilstrup, U. (2009). On the ability of the 802.11 p MAC method and STDMA to support real-time vehicle-to-vehicle communication. *EURASIP Journal on Wireless Communications and Networking*, *2009*, 5.

[5] Omar, H. A., Zhuang, W., & Li, L. (2013). VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs. *IEEE transactions on mobile computing*, *12*(9), 1724-1736.

printed by MegaPrint Inc. www.postersession.com