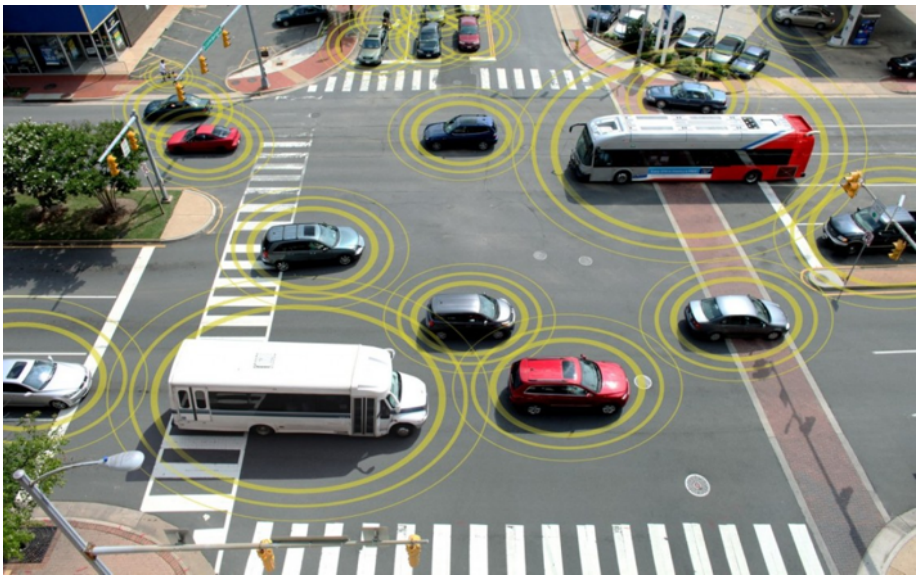
A18

Réseaux véhiculaires et robots

SR04 - GROUPE 3

COLOMB Oriane
WU Jitong
BOURGEON Theodore



SOMMAIRE

1. Introduction aux réseaux véhiculaires

A. Objectifs des réseaux véhiculaires

Quelques statistiques permettent d'illustrer les besoin et challenges liés aux voitures autonomes :

- Le nombre d'accidents de voitures par an excède les 5 millions,
- En 2011 aux USA, le nombre de décès sur les autoroutes s'élève à 32 000,
- Toujours en 2011 aux États-Unis, les embouteillages dans les grandes villes ont coûté :
    - 5,5 milliards d'heures de retard,
    - 11 milliards de litres de carburant gaspillés,
    - 25 milliards de kg de CO2.

En prenant en compte ces différents aspects, les réseaux véhiculaires sont des éléments clés d'un système de transport intelligent.
D'après le Département de transports des Etats-Unis, les réseaux véhiculaires ont le potentiel de résoudre plus de 79% des accidents n'impliquant pas des conducteurs aux facultés affaiblies (alcool, drogues, problèmes médicaux). A cette composante de **sécurité**, s'ajoute la notion de **temporalité** : gain de temps pour les usagers par la réduction des bouchons dans un premier temps, et une notion **financière** et **environnementale** dans un deuxième temps.

B. Une standardisation mondiale

C'est la première fois qu'un sujet est autant réfléchi par différents consensus mondiaux avant sa mise en application. Chaque région géographique possède ses propres contraintes et se doit de respecter des normes communes pour homogénéiser les technologies et les rendre compatible. Une organisation est en charge des avancées concernant les réseaux véhiculaires : **Intelligent Transportation Systems (ITS)**.

Différentes approches ont été prises en compte selon leurs régions géographiques mondiales. Elles ont chacune mené à des standardisations différentes :

- Japon :

Le Japon s'est principalement focalisé sur la mise en place des infrastructures liées au déploiement des réseaux véhiculaires comme l'infrastructure de l'ETC (Electronic Toll Collection). Une standardisation qui découle de ISO TC 204 sur les systèmes de transports intelligents : ARIB (Association of Radio Industries and Businesses), ISO, CALM, …

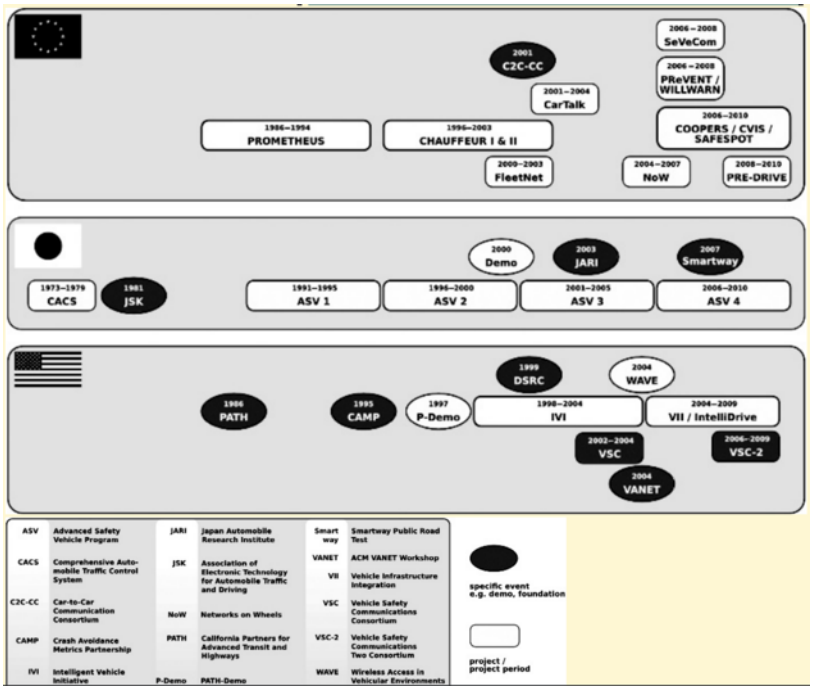
- Etats-Unis :

Cette standardisation est menée par l'industrie C2CCC (Car to Car Communication Consortia).
Les Etats-Unis ont définit un standard de la norme IEEE 1609 protocol suite (wireless access for vehicular environments).

- L'Union Européenne :

Elle a été impliquée principalement dans la définition des standard suivant :

- ETSI (European Telecommunications Standards Institute),
- ITS (Intelligent Transportation Systems),
- ISO (International Organization for Standardization),
- CALM (Continuous Air-interface Long and Medium range).



On peut résumer ainsi les principaux standards :

- **Dedicated Short-Range Communications (DSRC)**
  - Spectre de 75 MHz dans la bande 5,9 GHz (attribuée en 1999)
    - Gratuit et sous licence
  - Structuré en sept canaux de 10 MHz
    - 1 canal de commande et 6 canaux de service
- **IEEE 802.11p**
  - Définit les améliorations à 802.11 pour supporter les applications des réseaux véhiculaires
  - Approuvé en 2010 (groupe de travail formé en 2004)
- **WAVE (IEEE 1609 standards)**
  - Wireless Access in Vehicular environments
  - Mode de fonctionnement utilisé par les appareils 802.11p pour fonctionner dans la bande DSRC
  - La norme IEEE 1609.3 couvre la configuration et la gestion de connexion
  - La norme IEEE 1609.4 permet le fonctionnement des couches supérieures à travers des canaux multiples

C. WAVE (IEEE 1609 standards)

Les défis lancés par les réseaux véhiculaires de part leur grande échelle, leur très fort degré de dynamisme et leurs applications variées ont été étudiés par le groupe de travail IEEE 1609 pour développer une première version de l'architecture des protocoles des premières couches pour les réseaux véhiculaires. L'un des standards ainsi défini est le IEEE 802.11p basé sur les standards des réseau locaux sans fils détaillés par la suite.

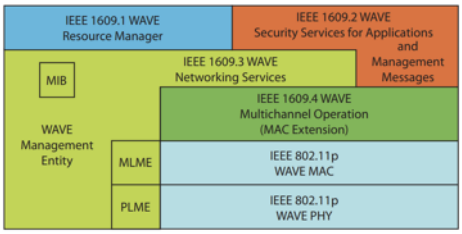
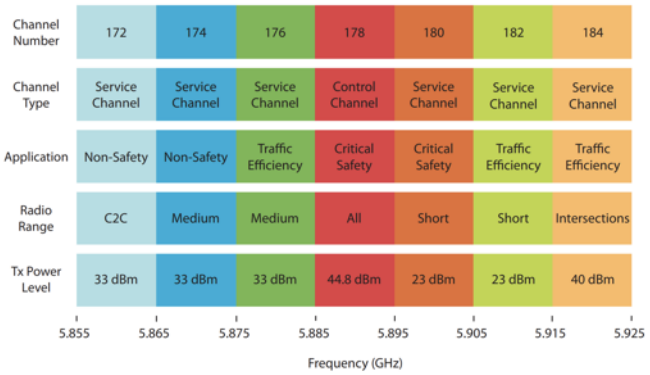


Fig. 1. The IEEE 1609 (WAVE) reference architecture and relationship to the IEEE 802.11p MAC and physical layers.

On constate que la norme IEEE 802.11p définit les couches WAVE PHY et WAVE LOWER MAC tandis que le reste provient de l'architecture de la norme IEEE 1609 :

- IEEE 1609.2 définit les services de sécurité pour les applications de messagerie et de gestion des messages dans les WAVE,
- IEEE 1609.3 définit l'interconnexion entre les appareils WAVE,
- IEEE 1609.4 se trouve juste au dessus de la couche 802.11p. Il s'occupe des aspects logistiques de la couche supérieure sans avoir connaissance des paramètres de la couche physique. Il définit les techniques de signalisation et les fonctions d'interfaces,
- Les couches IEEE 802.11p MAC 11p et PHY seront détaillées par la suite.

Le standard WAVE implique différentes fonctions réseaux et de gestion, notamment sur la sécurité, la gestion des ressources et les opérations multi-channels. Les fonctions de management pour les couche MAC et physique ont logiquement été séparées : MLME et PLME.
Différents canaux ont été définis dans la norme IEEE 1609.4 pour les opérations multichannel sur des fréquences différentes. Ils possèdent leurs propres caractéristiques dont la puissance maximale de transmission a été mise en place. Un spectre de 75 Mhz de bande passante, de 5850 a 5925 MHZ, a été dédié aux communications V2V et V2I par la FCC (Federal Communication Commission).



- **Channel 178** (5885 - 5895 Mhz): Pour le contrôle, les avertissements de service WAVE sont broadcastés ici afin d'indiquer comment accéder aux services des autres channels. Il possède la puissance maximale de transmission,
- **Channel 127** (5855 - 5865 Mhz) : Réservé aux communications de prévention de collisions. Il contient 3 types de message : Basic Safety Message, MAP message et Signal and Timing Message,
- **Channel 184** (5915 - 5925 Mhz) : Réservé aux communications de sécurité longue distance

D. IEEE 802.11p

Comme évoqué dans le standard IEEE 1609, le standard IEEE 802.p définit deux couches : IEEE 802.11p WAVE MAC et IEEE 802.11p WAVE Physique.

IEEE 802.11p WAVE MAC

En dessous des opérations multi-channels de la norme IEEE 1609, les schémas de priorité sont implémentés par la couche MAC IEEE 802.11p. Pour chaque canal, quatre AC (Access category, noté respectivement AC 0, AC 1, AC 2 et AC3) sont définis, où AC 3 possède la plus grande priorité. Ainsi les trames vont être placées dans des queues FIFO en fonction de leur priorité. Ces queues possèdent leur propre système de rétention.

Ce mécanisme est représenté dans la figure suivante :

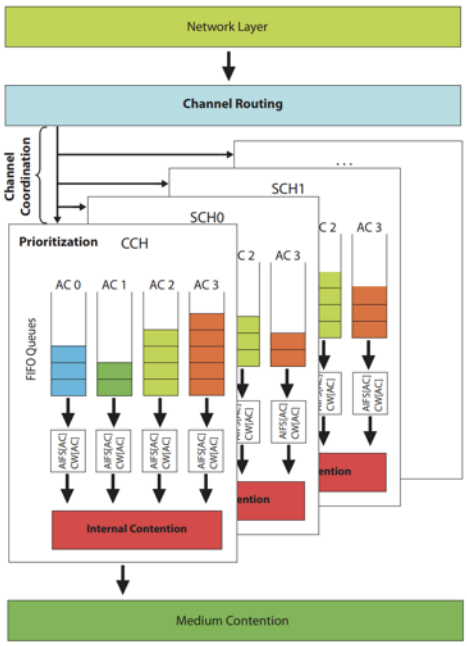


Fig. 3. Illustration of the relationships between the multichannel operation and the traffic prioritization with different access categories in the 802.11p MAC.

Pour chaque Access Category, dans chaque canal, des timers différents sont liés aux procédures de contention. Chaque trame “gagnante” va alors suivre le protocole CSMA/CA en plus.

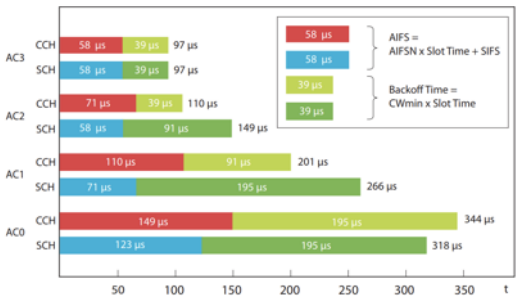


Fig. 4. The arbitration inter-frame space durations used in the EDCA settings for IEEE 802.11p for different channel types and access categories.

IEEE 802.11p WAVE Physique

La couche physique est basée sur OFDM et ressemble beaucoup au standard de la couche physique de 802.11a. Les différences notables sont :

- La bande passante est de 10 Mhz contre 20 Mhz dans 802.11a,
- La présence de changements de puissance de transmission et de changements de fréquences.

E. DSRC

Le DSRC (Dedicated short range communication) est un service utilisé dans les appareils équipés du WIFI 802.11p, notamment les communications inter-véhiculaires. Il s’agit d’un service de portée moyenne dans les systèmes de transports intelligents (ITS). Il supporte à la fois les problèmes de sécurité publique et les opérations de communications plus classiques entre les véhicules : prévention des collisions, amélioration de la mobilité et de l’environnement.

Comment cela fonctionne ?

- Entre deux véhicules :
    - Chaque véhicule envoie en broadcast les informations sur son état dans des messages BSM (Basic Safety Message) toutes les 0.1 secondes sur 360 degrés en utilisant IEEE 802.11p.
    - Les récepteurs construisent un modèle de la trajectoire de chaque voisin en évaluant la menace potentiel pour le véhicule hôte : avertissement du conducteur ou prise de contrôle lorsque la menace devient forte.

- Entre un véhicule et une infrastructure, plusieurs messages peuvent être envoyés : SPaT message (signal de phase et temporel), MAP message (Structure de l’intersection), et autres informations concernant la vitesse, restriction de taille, gel, ...

Table 2: Layered architecture for DSRC.

Safety applications		Nonsafety Applications
Transport and network layer IEEE 1609.3		**Transport layer** TCP/UDP
Security IEEE 1609.2		**Network layer** IPv6
	LLC sublayer IEEE 802.2	
	MAC sublayer extension IEEE 1609.4	
MAC sublayer PHY layer		IEEE 802.11p

Quelques mises en situations :

- Un message de collision frontal si deux véhicules s'approchent l'un de l'autre,
- Un message de freinage d'urgence pour prévenir les véhicules environnants si les conditions ne permettent pas une vision directe de la situation (Exemple : derrière un camion),
- Un message lors d'un déplacement, lorsqu'un véhicule se trouve dans un angle mort :
    - Message de danger lorsqu'il s'agit de notre véhicule,
    - Message d'avertissement lorsqu'il s'agit des deux autres.
- Un message d'interdiction de dépassement ou d'avertissement de croisement d'intersection quand la visibilité ne permet pas de voir l'autre véhicule.

2. Applications et besoins des réseaux véhiculaires

A. Applications et cas d'usages

i. Sécurité routière active

Constat : Une grande partie des accidents sont associés aux intersections dans des collisions frontales, latérales ou arrières.
Objectifs : Réduire la probabilité d'accidents de la route et le nombre de pertes humaines.
Les applications apportent de l'information et de l'assistance aux conducteurs pour éviter ce genre de collisions. Le transfert de données entre les véhicules (V2V) et des unités de gestion sur le bord de la route (V2I) sont nécessaires pour prédire certaines collisions : la position des véhicules, la position du croisement, la vitesse, les distances de sécurités mais aussi l'état de la route et la dangerosité de certaines sections.

On distingue alors plusieurs axes :

- Alerte d'intersection : La présence d'un véhicule en approche d'une intersection est signalé pour réduire le risque de collision latérale,
- Assistance au changement de voie : Lors d'un dépassement avec un champs de vision réduit,
- Avertissement de dépassement : Communication de l'information entres les différents véhicules,
- Alerte de collision frontale : Signalement des véhicules roulant à contre-sens,

- Véhicules d'urgence : Avertissement pour libérer une voie d'urgence,
- Pré-crash : Dans le cas d'une collision inévitable, il y a un échange d'informations pour optimiser l'utilisation des équipements du véhicule et ainsi limiter l'effet de l'accident,
- Manœuvre de fusion de jonction : Négociation des véhicules pour l'insertion,
- Avertissement d'un freinage fort,
- Détection du non-respect des règles de circulation,
- Avertissement de présence de véhicules arrêtés,
- Condition du trafic et son évolution,
- Risque de collision entre deux véhicule ne pouvant pas communiquer : Envoie de l'information à tous les véhicules autour,
- Notifications d'éléments ponctuels : Travaux, véhicule sur le bas-côté,
- Avertissement de perte de contrôle d'un véhicule.

ii. Optimisation du trafic et gestion

Objectifs : Améliorations du trafic (débit, coordination, assistance par la récupération de messages) pour gérer deux aspects :

- Vitesse : Assistance du conducteur pour améliorer la fluidité de sa vitesse et éviter les bouchons,
- Coopération de navigation : Améliorer l'efficacité des routes en gérant le trajet des différents véhicules.

iii. Informations et divertissement

Objectifs :

- Locaux : transmission d'informations sur des services locaux,
- Globaux : Informations provenant d'internet comme les assurances, les zones de parking, etc..

B. Classification des besoins

Les besoins des réseaux véhiculaires proviennent de l'étude avancée des cas d'usages et des applications. On peut classifier ces besoins de la façon suivante :

1. **Stratégiques** : Niveau de déploiement du réseau comme le taux minimum de pénétration (taux d'utilisateurs) et stratégies définies par les gouvernements et les commissions.

2. **Économique** : Valeur économique, plus-value utilisateur.

3. **Système** :
   - Capacité de communication radio : Portée, canaux de fréquence radio, bande passante, débit, robustesse, niveau de compensation des erreur de propagation des signaux,

- Capacité de communication réseaux : Mode de communication (unicast, broadcast, multicast, geocast), agrégation de données, gestion de la congestion, gestion des priorités, adressage IPv4 et IPv6,
- Positionnement des véhicules : Global Navigation Satellite System (GNSS), Global Positioning System (GPS), local geographical map,
- Sécurisation des communications : Respect de la vie privée et de l'anonymat, intégrité et confidentialité, résistance aux attaques externes, authenticité des données (communications, données et systèmes).

4. **Performances** : Communication, temps de latence maximal, fréquence de mise à jour des données, précision de la position, dépendance matérielle, taux d'erreur, zones non couvertes, vérification des messages.

5. **Organisationnels** : Nommage et adressage, IPv4 et IPv6 schéma d'allocation d'adresses, interopérabilité entre ITS, organisation indépendante pour assurer les besoins de sécurité.

6. **Légaux** : Le respect de la vie privée.

7. **Standardisation et certifications**: Systèmes, ITS, conformité des tests des biens et des services, gestion des risques.

Ici sont listées les différents besoins, leur moyen de communication associé avec les fréquences minimales de transmissions ainsi que le temps de latence critique. Les technologies associées devront être établies dans le respect de ces différentes informations.

TABLE I
ACTIVE ROAD SAFETY APPLICATION REQUIREMENTS

Use case	Communication mode	Minimum transmission frequency	Critical latency
Intersection collision warning	Periodic message broadcasting	10 Hz	< 100 ms
Lane change assistance	Co-operation awareness between vehicles	10 Hz	< 100 ms
Overtaking vehicle warning	Broadcast of overtaking state	10 Hz	< 100 ms
Head on collision warning	Broadcasting messages	10 Hz	< 100 ms
Co-operative forward collision warning	Co-operation awareness between vehicles associated to unicast	10 Hz	< 100 ms
Emergency vehicle warning	Periodic permanent message broadcasting	10 Hz	< 100 ms
Co-operative merging assistance	Co-operation awareness between vehicles associated to unicast	10 Hz	< 100 ms
Collision risk warning	Time limited periodic messages on event	10 Hz	< 100 ms

TABLE II
SPEED MANAGEMENT PERFORMANCE REQUIREMENTS

Use case	Communication mode	Minimum transmission frequency	Critical latency
Regulatory contextual speed limit notification	Periodic, permanent broadcasting of messages	1-10 Hz depending on technology	Not relevant
Green light optimal speed advisory	Periodic, permanent broadcasting of messages	10 Hz	< 100 ms

TABLE III
CO-OPERATIVE NAVIGATION PERFORMANCE REQUIREMENTS

Use case	Communication mode	Minimum transmission frequency	Critical latency
Electronic toll collection	Internet vehicle and unicast full duplex session	1 Hz	< 200 ms
Co-operative adaptive cruise control	Cooperation awareness	2 Hz (some systems require 25 Hz [20])	< 100 ms
Co-operative vehicle-highway automatic system (platoon)	Cooperation awareness	2 Hz	< 100 ms

3. Différents types de réseaux

Afin d'expliquer les réseaux véhiculaire, nous devons les mettre en opposition avec les réseaux mobiles.

A. Réseaux Mobiles ou MANETs (Mobile Ad hoc NETworks)

Dans un premier temps nous allons expliquer la différence entre les réseaux Ad hoc et les autres. Contrairement au réseau internet classique, les réseaux mobile ad hoc ont :

- Un réseau flat, sans infrastructure particulière,
- Il utilise la communication radio avec un range moyen,
- Chaque appareil est à la fois un routeur et une machine,
- Chaque nœud est autonome,
- La topologie réseau est dynamique,
- Il nécessite peu d'énergie et de ressources de calculs.

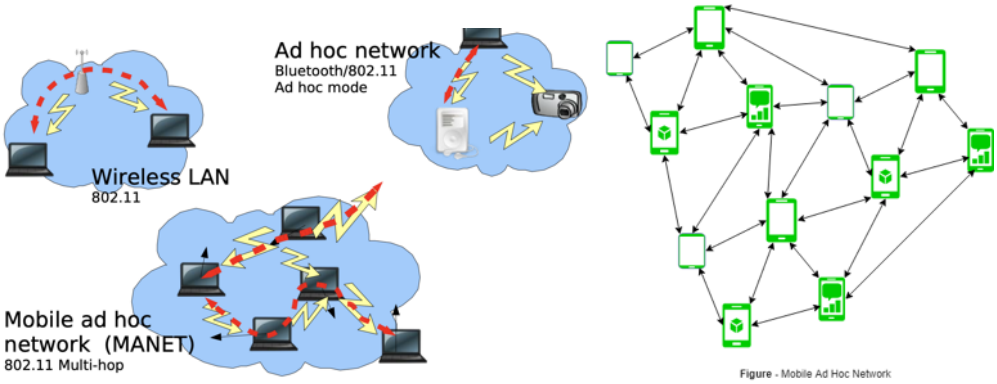


Figure - Mobile Ad Hoc Network

Les principales différences avec les réseaux câblés et les réseaux radio sont les suivantes :

- La variabilité du rapport signal/bruit,
- La possibilité de transmettre sur des distances différentes,
- CSMA (Carrier Sense Multiple Access) : Écoute d'un support à accès multiples,
- Contestation des canaux de communications,
- Blocages et interférences .

Dans les réseaux Ad hoc, pour un réseau flat, le routage est très important : on doit être capable de trouver des chemins de bout en bout pertinents, le réseau doit être en mesure de s'adapter en fonction de sa taille, ne pas boucler et maintenir des routes.
Pour cela, il se base sur trois protocoles de routages principaux :

- **Réactif** : Vue partielle du réseau ou seulement des routes actives où les mises en cache sont connues. Cela garantie une grande réactivité aux changements de topologie.
- **Proactif** : Vue globale du réseau par envoi périodique d'informations, une route est disponible en fonction du besoin. La convergence des informations de proche en proche est lente.
- **Hybride** : Un intermédiaire entre les protocoles réactifs et proactifs.

Concernant la standardisation et l'avancée des recherches, un groupe de travail de l'IETF réfléchit à ces différentes questions et propose des standards de routage MANET depuis 1995 en se basant sur des protocoles : OLSR (Optimised Link State Routing), AODV (Ad hoc On-demand Distance Vector) et DSR (Dynamic Source Routing).
Hormis le routage, des recherches sur la sécurité, les mécanismes incitatifs et l'interface avec internet sont également en cours.

Les applications principales des réseaux MANETs sont :

- **Militaire** : Dans des terrains inconnus, pour des distances limitées, basé sur des infrastructures destructibles,
- **Humanitaire** : Notamment lors de catastrophes naturelles à des fins de recherche et de sauvetage,
- **Commerciales** : Réseaux communautaires, réseaux locaux personnels et jeux ad hoc.

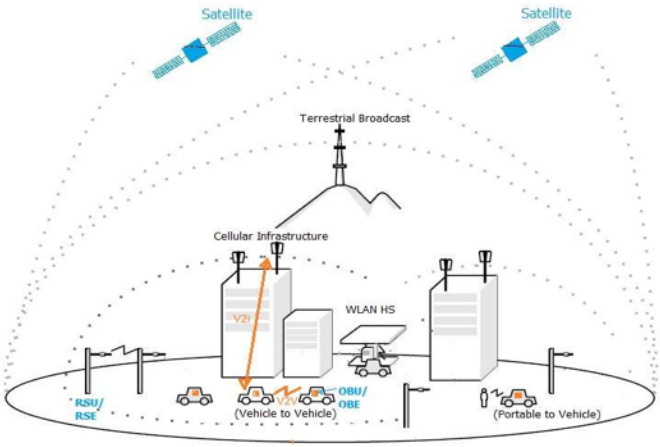
Les réseaux véhiculaires pourraient être associés à des réseaux mobiles, mais ils s'en distinguent par des besoins et des contraintes différentes. Nous allons à présent, après avoir présenté les MANETs, nous focaliser sur les VANETs (Vehicular Ad hoc NETwork), dans lesquels les noeuds se déplacent beaucoup plus rapidement, avec des directions fixes dans un domaine beaucoup plus étendu.

B. Réseaux Véhiculaires ou VANET (Vehicular Ad hoc NETwork)

Les systèmes de transport intelligents (STI) désignent les applications des nouvelles technologies de l'information et de la communication dans le domaine des transports. De nouvelles fonctions permettent :

- D'appréhender l'environnement grâce à des capteurs,
- Communiquer avec les autres véhicules grâce à des interfaces radio sans fil ou 3G,
- Traiter ces informations et prendre des décisions sur le comportement du véhicule grâce à un calculateur embarqué.

Les réseaux de véhicules doivent répondre à plusieurs défis : une topologie variante (d'une densité très faible à très forte), des modifications des signaux en provenances des autres véhicules (bâtiments) et la connectivité. Les mouvement directionnel à grande vitesse et de grande envergure entraîne une difficulté pour trouver des routes de bout en bout.



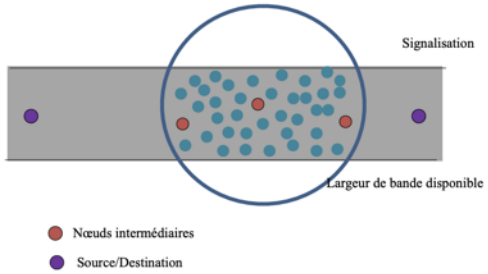
Les interfaces radio permettent aux véhicules de communiquer entre eux (**Vehicle-to-Vehicle Communication, V2V**) ou avec des unités installées au bord de la route selon des communications **V2I (Vehicle-to-Infrastructure Communications)**. Dans le domaine de la sécurité routière, les communications entre véhicules peuvent étendre la portée de détection des capteurs radar embarqués. Par exemple, un véhicule qui détecte la présence de verglas pourra communiquer cette information aux véhicules qui le suivent.
Des services nécessitent une connexion à Internet, on parle alors de communications **V2V2I (Vehicle-to-Vehicle-to-Infrastructure)**. Une architecture V2V2I est donc constituée de deux parties, d'une part des réseaux ad hoc de véhicules ou VANET et d'autre part, un réseau mobile classique. Une telle architecture présente un double avantage. D'une part, les VANET étendent la couverture du réseau d'infrastructure à des zones non couvertes et d'autre part, le réseau d'infrastructure interconnecte les VANETs entre eux et leur permet l'accès à des services de type Internet.

Les réseaux ad hoc de véhicules sont un cas particulier des réseaux ad hoc mobiles caractérisés par une forte dynamique due à la mobilité rapide des véhicules. Cependant, le réseau ad hoc de véhicules souffre d'une connectivité discontinue et d'une capacité limitée.

Dans les VANETs, à la fois pour une communication V2V et V2I, le WIFI est utilisé selon les spécifications **802.11p**. Ainsi, nous pouvons redéfinir le VANET : c'est l'ensemble réseau formé par les machines

Les communications Véhicule à Véhicule - V2V

Comme énoncé précédemment, le principe des communication V2V est la communication entre deux véhicules. De nombreux défis dues aux caractéristiques du VANET sont alors à relever. Basé sur la norme 802.11p, l'objectif est de faire communiquer des véhicules les uns les autres en réduisant au maximum les délais tout en assurant la fiabilité.
En se basant sur de nombreux algorithmes, lors de congestion de trafic, l'idée est d'utiliser au sein de ce réseau ad hoc, différents nœuds pour faire transiter le plus rapidement l'information tout en restant à portée.



Les communications Véhicule à Infrastructure - V2I

Face à des scénarios de faible trafic ou lorsque seulement peu de véhicules sont équipés avec 802.11p, il est nécessaire de déployer de nouveaux moyens : soit dans le domaine du transport et des transmissions, soit par le biais d'infrastructures faisant le pont entre les véhicules. Dans cette optique, un déploiement d'infrastructures le long des routes, aux intersections, dans des zones à risques est complémentaire à la communication V2V. On instaure donc une communication entre véhicule et infrastructure (V2I).

Les autres communications

Il existe d'autres types de communications véhiculaire :

- Les communications intra-véhiculaire, plus ou moins importante dans les VANETS. L'objet de la recherche est axée sur la détection des performances, par exemple sur la fatigue du conducteur ou son attention, deux éléments critiques pour la sécurité routière,
- Les communications V2B utilisant les réseaux mobiles tel que la 3G ou la 4G (Vehicle-to-broadband cloud). Les réseaux itinérant contiennent plus d'informations sur le trafic et sur les informations de divertissement. Ils sont donc utiles dans l'assistance du conducteur et le suivi des véhicules.

Ce graphique regroupe les différents moyens de communications, leurs intérêts et les atouts de leur combinaisons :

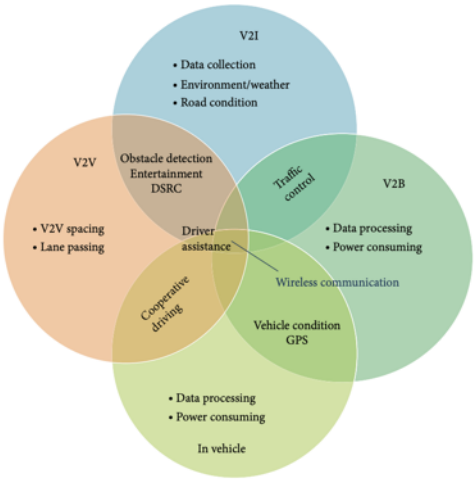


FIGURE 3: Key functions of each communication type.

4. Comparaison des différentes technologies disponibles

Technologies classiques

Nom	**Portée Max**	**Taux de Transfert**	**Fréquence**	**Mobilité**	**Infrastructure**	**Applications Principales**
Bluetooth	10 m	> 721 Kbps	Non	Très lent	Non	ETC Usage intravéhicule
RFID	10 m	500 Kbps	Non	Lent	Non	ETC Identification du véhicule
WLAN : Wifi	100 m (extérieur)	11 ou 54 Mbps	Non	Moyen	Non	Faible exigence, bas coût et usage général
WPAN : ZigBee	300 m (extérieur)	250 Kbps	Non	Moyen	Non	
DSRC	1 km	27 Mbps	Oui	Très vite	Personnalisable	Sécurité Fluidité du trafic et efficacité énergétique Confort de conduite
3G : ULTRA-TDD	1 km	144 Kbps (véhicule) 384 Kbps (extérieur) 2 Mbps (intérieur)	Non	Vite	Oui	Fluidité du trafic et efficacité énergétique Confort de conduite
4G : WiMAX	51 km	40 Mbps (statique) 14 Mbps (mobile)	Personnalisable	Vite	Oui	
4G : LTE	100 km	100 Mbps (statique et mobile)	Personnalisable	Très vite	Oui	

5G : La nouvelle génération des communications mobiles

Le nombre important d'appareils mobiles, la grande quantité de données et le besoin en débit ont menés à repenser le fonctionnement des réseaux actuels de communications. La prochaine génération (5G) est attendue pour solutionner ces différents points notamment pour les futurs systèmes de transport intelligent.
Les réseaux 5G sont caractérisés par 3 fonctionnalités :

- Une connectivité universelle,
- Un temps de latence extrêmement bas,
- Un débit de transfert très haut.

En effet, les architectures VANETs actuelles ne peuvent pas, dans des situations de hautes congestions ou de mobilité extrême, atteindre les minima requis en terme de temps de latence.

La prochaine architecture vanets

Pour supporter ces contraintes plusieurs mécanismes fonctionnent simultanément :

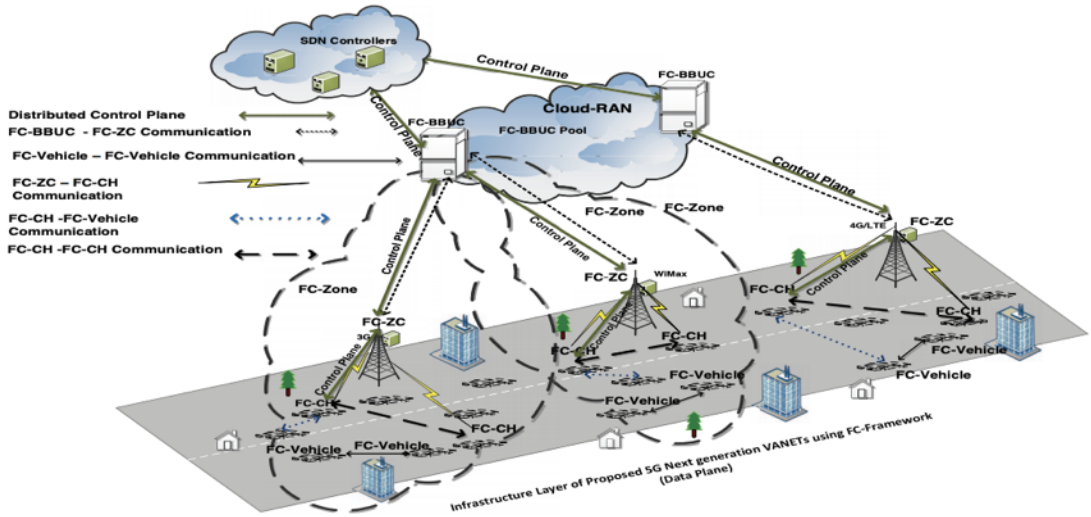


Fig. 1: Topology Structure of 5G Next generation VANETs using SDN and Fog Computing (FC) Framework

- **SDN controller :**
  Composant principal, le contrôleur SDN est responsable du management du réseau, de l'allocation des ressources, de la gestion des règles et de la mobilité. Il gère également l'orchestration du Fog tout en analysant le réseau et en prétraitant les données.

- **Fog Computing** (FC) :
  - Fog Computing BBU Controllers (FC-BBUC) : Il contrôle plusieurs FC-ZC et est responsable, entre autre, du traitement des paquets. Il collecte les informations des différents FC-ZC et prend des décisions sur l'acheminement pour réduire la surcharge. Il joue ainsi un double rôle: plan de données et outils de contrôle.
  - Fog Computing-Zone Controllers (FC-ZC) : Il s'agit des centres de calculs des infrastructures du réseaux sans fil. Dans ce cas, les zones correspondent à des groupes de véhicules.

- Fog Computing-Cluster-heads (FC-CH) : Chaque zone est subdivisée dans des clusters FC-CHs contrôlés par le même FC-ZC.
- Fog Computing-Vehicles (FC-Vehicles) : Ils fonctionnent comme des utilisateurs terminaux et sont acteur des communications V2V et V2I.

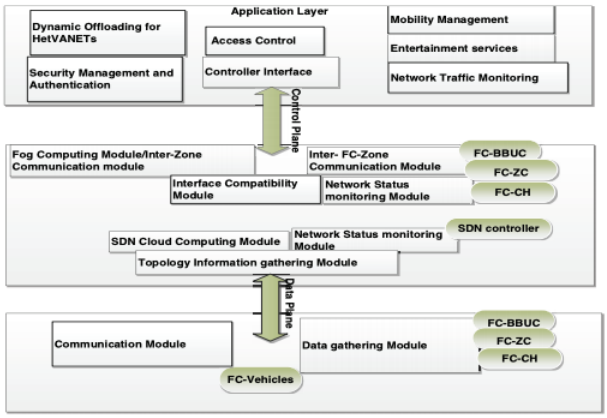


Fig. 3: Logical Structure of proposed 5G Next generation VANETs

Il existe d'autres architectures possibles soutenant la 5G et améliorant les VANETs mais celle-ci est représentative des challenges et infrastructures nécessaire à la mise en place d'un réseau véhiculaire.

5. Challenges et solutions

A. Algorithme de transmission / Routage

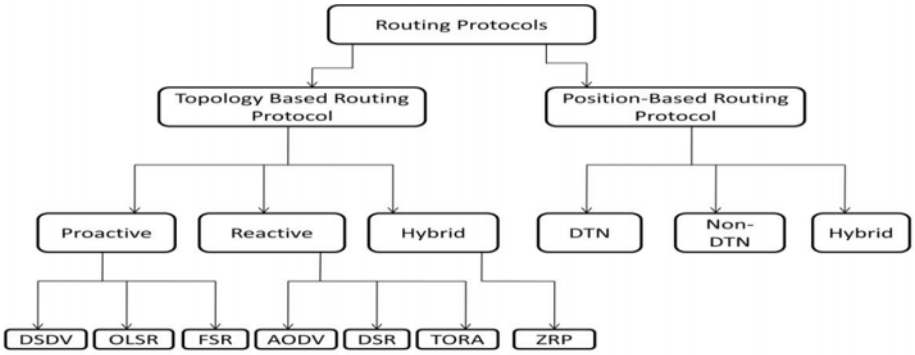


Fig. 2. VANET Routing Protocols [35]

1. Routage non-géographique

Voici une liste non-exhaustive d'algorithmes de routage non-géographique des MANETs qui sont transposables aux VANETs :

- Notion de loop-free dans le protocole de routage DSDV,
- Notions de "réactif" et de "non-redondance" de AODV,
- Notion de "routage par la source" du protocole de routage DSR,
- Notion de "link-reversal algorithm" dans TORA,
- Mécanisme "basé sur zone/cluster" dans ZRP.

2. Routage géographique

Le premier défi des algorithmes de routage géographique est la localisation du véhicule. Les GPS sont assez répandus, mais pas tous les véhicules en sont équipés (ou équivalent). De plus, si le nombre de satellites est insuffisant (bâtiments gênants), on peut collecter une position imprécise.

Les algorithmes de routage géographique nécessitent normalement qu'un nœud dispose de 3 informations :

- Sa propre position,
- Les positions des nœuds voisins,
- La position du nœud destination.

Il existe plusieurs services civiles qui peuvent aider un nœud à obtenir sa position :

- **DGRS** : Corrige les positions du GPS en soustrayant les erreurs obtenues par les stations de référence,
- Map matching : Utilise les connaissances de la carte géographique pour améliorer les positions,
- Cellular Localization : Corrige les positions à l'aide de l'infrastructure des mobiles,
- **Image/video processing** : Fournit les positions en utilisant les systèmes de sécurité routiers,

- **Indoor infrastructure assist** : Utilise les caractéristiques de propagation du signal pour un environnement intérieur,
- **Dead reckoning** : Calcule la position courante à partir de la dernière position connue,
- Relative distributed ad hoc localization : Estime la distance par les positions connues d'autres noeuds.

Une grandes partie de ces systèmes repose sur des infrastructures.
Les systèmes en verts reposent sur une approche globale. Ils sont plus précis que les autres.
Le système en bleu peut être réalisé sur un noeud indépendamment des autres. Il est moins précis sur une longue distance

La position des nœuds voisins est obtenue par un simple broadcast périodique. De plus, dans certaines stratégies, il n'est pas nécessaire de connaître la position des nœuds voisins à l'avance.

Le problème principal est donc la découverte de la position du nœud destination. On peut alors se trouver dans 2 situations :

- Le nœud source peut obtenir la position du nœud destination par l'infrastructure routière (Cas favorable).
- Le nœud source doit déclencher un *flooding* pour obtenir la position du nœud destination via un nœud du réseau qui peut l'atteindre (Cas complexe). Deux techniques sont envisageable dans cette situation :
    - Localisation basée sur le flooding,
    - Localisation basée sur la mise à jour et l'interrogation.

Localisation basée sur le flooding :
Le protocole DREAM (Distance Routing Effect Algorithm for Mobility) est une technique de flooding : un nœud maintient une table des positions des nœuds qu'il peut entendre et il essaie d'envoyer sa position aux nœuds qu'il peut atteindre.

Pour contrôler la surcharge, DREAM considère 2 paramètres :

- La mobilité : Un nœud qui se déplace plus vite va diffuser plus fréquemment sa position.
- La distance : Si 2 nœuds sont à des distances différentes d'un nœud donné, le nœud le plus éloigné semblera se déplacer plus lentement que le nœud le plus proche (même si les 2 se déplacent à la même vitesse).

Le récepteur du paquet calculera l'effet de distance, comparera au nombre de sauts du paquet et décidera si le paquet est éliminé.

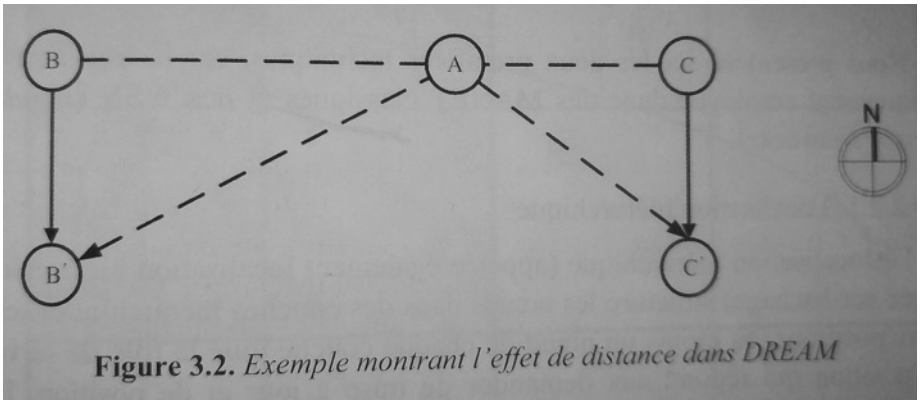


Figure 3.2. *Exemple montrant l'effet de distance dans DREAM*

Dans la figure, pour le nœud A, le nœud B semblera se déplacer moins vite que le nœud C.

Localisation basée sur la mise à jour et l'interrogation :
Cette méthode comporte 2 processus :

- La mise à jour de la position : Envoie des informations relatives à la position à un sous-ensemble de nœuds appelés serveurs de position,
- La demande de position : Recherche des serveurs de position afin d'obtenir la position du nœud destination.

Dans le VANET, il existe 2 stratégies différentes applicables à cette méthode :

- La localisation hiérarchique,
- La localisation basée sur le quorum.

Localisation hiérarchique ou localisation hiérarchique basée sur le hachage :
Cette technique structure les nœuds dans des couches hiérarchiques selon leurs positions. Au moins un nœud de chaque couche joue le rôle de serveur de position qui répond aux demandes de mise à jour et de position. Ce type de localisation permet de réduire le surcoût de la localisation et garantit l'extensibilité du réseau.

Le protocole GLS (Grid's Localization Service), qui doit encore valider sa robustesse, est un exemple de ces caractéristiques appliquées aux VANETs.

Il s'agit d'un protocole hiérarchique décentralisé qui peut prendre en charge les nœuds à mobilité lente avec peu de surcoût de localisation. Si les nœuds connaissent leur position GPS, ils se sont mis d'accord pour une racine commune de la hiérarchie.
Une couche du réseau GLS est un carré d'ordre n (1, 2, …).
Dans un carré d'ordre 1, chaque nœud doit être sous la couverture de communication de tous les autres et la distance maximale de communication dans un carré d'ordre 2 est supposé égale à 2 sauts.
Plusieurs carrés d'ordre n forment un carré d'ordre n+1 qui est la couche suivante.
La mise à jour de position et la demande de la position du nœud destination ne repose pas complètement sur la division géographique.

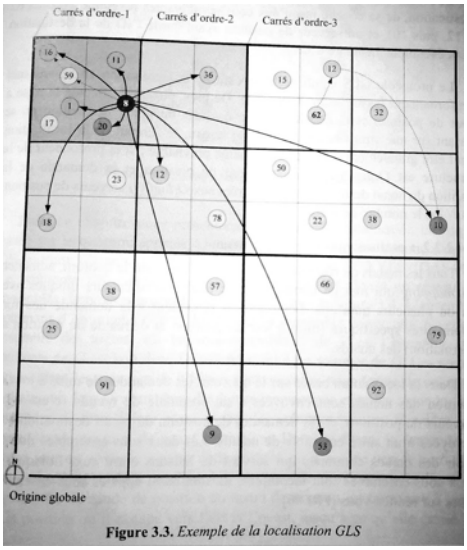


Figure 3.3. *Exemple de la localisation GLS*

Localisation basée sur le quorum :

Tous les nœuds admettent un mapping qui met en correspondance leurs identificateurs uniques avec un ou plusieurs quorums. Leurs quorums répondent à la demande des fonctionnalités spécifiques des nœuds.

Les demandes de mise à jour de position des nœuds sont envoyées à un ensemble de nœuds et les demandes de position du nœud destination sont envoyées à un autre ensemble de nœuds.

Les 2 sous-ensembles doivent avoir des nœuds communs qui servent de liaisons entre eux.

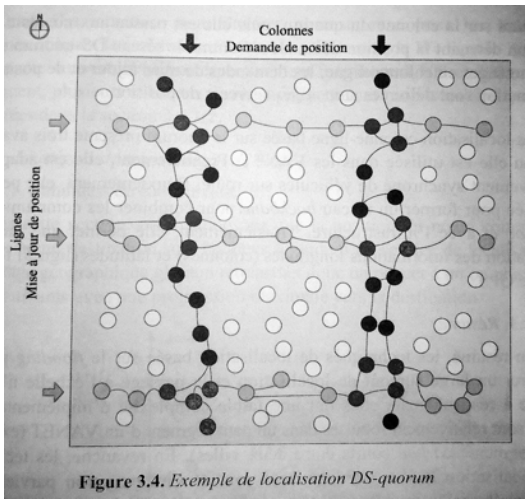


Figure 3.4. *Exemple de localisation DS-quorum*

Pour résumer, ces 2 types de localisation basée sur le flooding peuvent générer un large surcoût de localisation et le passage à l'échelle n'est pas facile à réaliser, mais ils ont une faible complexité d'implémentation et sont relativement robuste pour un petit segment de VANET.

Une fois la localisation de l'émetteur, des nœuds voisins et de la destination acquise, plusieurs algorithmes de routage sont envisageables :

- Routage unicast glouton,
- Routage Geocast (Multicast),
- Routage DTN (Delay Tolerant Network),

- Routage basé sur une carte.

Routage unicast glouton :

Problème rencontré :

Le problème rencontré avec ce type de routage est qu'il échoue lorsque la transmission se retrouve en situation de zone vide, où aucun nœud n'est plus proche de la destination que le réexpédier lui-même. Des zones vides peuvent fréquemment apparaître dans le VANET, car les véhicules ne sont pas uniformément distribués.

Solution :

Il existe des solutions de recouvrement à ce problème.

Notamment, le Perimeter Routing permet la livraison d'un paquet en exigeant seulement les informations des nœuds voisins à un saut, si une route de bout en bout existe.

Des algorithmes de recouvrement utilisant la techniques du Perimeter Routing existent et sont relativement intuitifs à comprendre :

- FACE-1 :

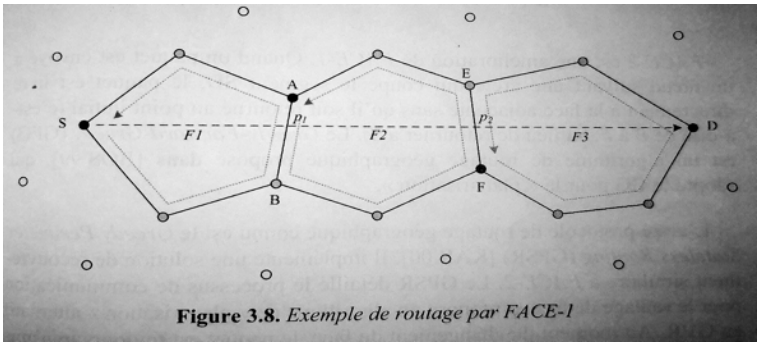


Figure 3.8. *Exemple de routage par FACE-1*

- FACE-2 :

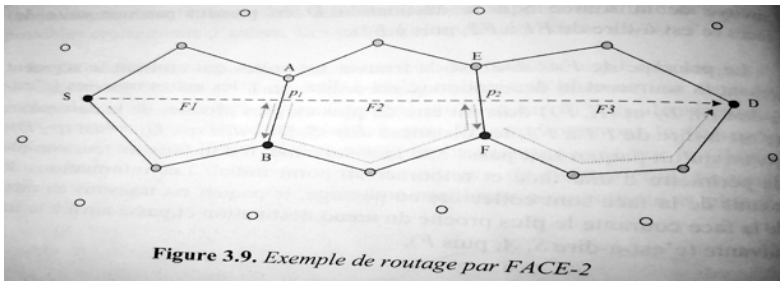


Figure 3.9. *Exemple de routage par FACE-2*

Routage Géocast :

Les étapes de transmission du Géocast sont similaires à la transmission basée sur la régulation, mais la destination dans le geocast est le plus souvent un cluster géographique. Dans le cas où la destination est un nœud seul, le mode de transmission peut être changé en unicast quand les paquets arrivent à la frontière du cluster contenant le nœud destination.

Routage DTN :

Le Delay Tolerant Network est un cas extrême de MANET. Le DTN se distingue par le fait qu'il considère que la connexion de bout en bout entre la source et la destination est fréquemment rompue à cause du partitionnement du réseau.

Routage basé sur une carte :
On peut le considérer comme un routage VANET semi-géographique. Il n'emploie pas directement les mécanismes d'interrogation saut à saut et de transmissions présentés précédemment, mais il travaille avec une carte routière pour le calcul du plus court chemin. Dans le cas des métropoles, il est pratique et de manière générale donne de meilleurs résultats qu'une technique sans carte routière.

B. Priorisation et congestion

Dans le cas des VANETs, la gestion du problème de congestion est une priorité.
Les applications de sécurité routière active font par exemple face à un problème.
Dans ce type d'application, il est commun de trouver une nouvelle couche facilities située entre la couche application et transport. Son rôle est de garder une image d'ensemble du réseau.

On dénombre 2 types de messages dans ces applications :

1) **CAM** : Ils fonctionnent comme une conscience coopérative. Ces messages sont envoyés de manière périodique. On les appelle aussi "message balise" ou "beacon". Ils transportent des informations sur l'état général du véhicule (vitesse, ralentissement, …).
   Les besoins applicatifs font que le beacon n-1 est supprimé dès l'arrivée du beacon n, afin d'éviter la propagation de données obsolètes. Ce mécanisme est appelé "back-off".
2) **DENM** : Ces messages sont utilisés pour communiquer sur un danger potentiel. Ils sont diffusé en broadcast et c'est la couche facilities qui fait le tri.

Dans ce type de réseau, nous faisons face à 2 problèmes :

1) Lorsque les messages de broadcast représentent plus de 50% du trafic, le comportement du réseau n'est pas un comportement classique.
2) Si nous prenons le cas des signaux radios (par exemple), ceux-ci sont capables d'émettre sur 1 km. Dans des conditions de circulation normale, sur une autoroute 2*2 voie, notre réseau serait formé de 160 voisins, ce qui est bien supérieur à ce que l'on trouve généralement.

Pour être résolu, ces problèmes nécessitent donc de gérer la congestion sur un réseau.

Dans le Traité Réseaux et Télécoms "Réseaux Véhiculaires : modèles et algorithmes", 5 solutions sont envisagé à ce problème :

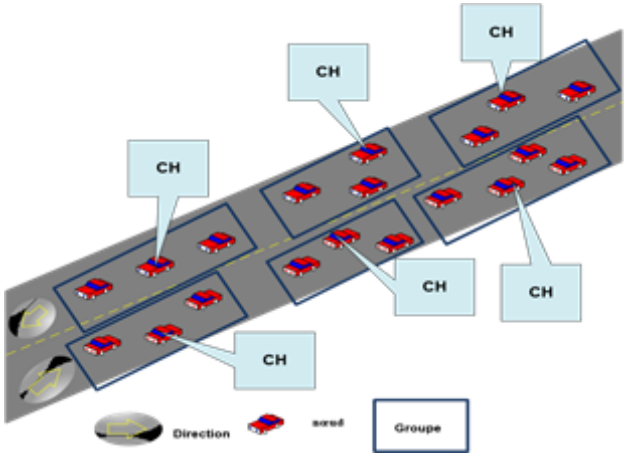
1) Diminuer la fréquence d'émissions des beacons pour désaturer le réseau,
2) Augmenter le débit d'envoi pour que le taux d'occupation du canal diminue,
3) Contrôler la puissance de transmission (jouer sur le nombre de stations cachées) afin d'augmenter la réutilisation spatiale
4) Diminuer la taille de la fenêtre de contention (avec pour impact une hausse de la probabilité de collision),
5) Jouer sur le mécanisme de détection de la porteuse (carrier serie).

C. Formation de clusters

Dans les VANETs, le clustering est une technique de regroupement des nœuds du réseau de manière hiérarchique suivant certains paramètres qui rendent le réseau plus robuste et évolutif. Les nœuds des VANETs se caractérisent par leur grande mobilité. Les nœuds qui se situent à la même proximité géographique n'ont pas nécessairement le même modèle de mobilité. Par conséquence, le regroupement VANET prend en compte le degré de différence de vitesse entre les nœuds voisins pour produire un structure relativement stable. Les clusters sont des sortes de groupes virtuels qui ont été formés par un algorithme de clustering.

1. Protocole de routage de clustering

Chaque groupe a au moins un Cluster-Head (CH) qui est sélectionné ou élu par d'autres membres du groupe Cluster-Member (CM).
La taille du cluster varie d'un groupe à l'autre et dépend surtout de la portée de transmission du dispositif de communication sans fil qu'utilise un nœud.
Le filtrage de certains algorithmes de clustering peut empêcher des nœuds de rejoindre un cluster. Parmi les algorithmes les plus utilisés, on trouve le filtre de la direction du mouvement. Un CM ne peut pas rejoindre un cluster qui se déplace dans la direction opposée. Chaque CN peut communiquer directement avec son CH et deux CM différents peuvent communiquer entre eux directement ou dans le pire des cas, via leur CH.



2. Comparaison des solution de clustering

L'objectif principale de clustering est de rendre le topologie globale moins dynamique. Pour calculer la stabilité des groupes des nœuds, nous avons la formule suivante :

$$Stabilité = facteur\ de\ fiabilité + Vitesse\ moyenne + la\ différence\ de\ distance$$

Le table ci-dessous compare brièvement les différent algorithme de clustering :

	Métrique	Localisation	Commentaire
MOBIC (mobility metrics clustering)	Mobilité relative, ID le plus bas.	……	Adaptable à différents niveaux de mobilité.
AMACAD	Emplacement, la vitesse relative et destination final.	GPS, les statistiques routières.	Adaptable à différents densité des groupes.
APROVE (utilise Affinity Propagation)	Vitesse, responsabilité, disponibilité, position.	……..	La taille de message Hello augmente en fonction de la densité de trafic.
VWCA (utilise une métrique complexe)	Méfiance, la direction.	Emplacement connu.	……
HCA	Zone de couverture.	N'est pas utilisable.	N'améliore pas la stabilité des nœuds.
C-DRIVE	Direction, densité.	……	La mobilité dépend de nombre de cluster-Head.
Fang et al.	La taille moyenne des groupes, variation moyenne des cluster-heads.	……	Utilisation d'information du trafic permis plus de stabilité.

D. La conception de SDN (Software-defined network) VANET

Le SDN (Software-defined network), proposé en 2015, est un nouveau challenge pour améliorer les VANETs. Il permet de résoudre certains problèmes des VANET :

- L'inflexibilité de l'architecture,
- Le nombre de véhicules très élevé,
- La diversité (hétérogénéité) des flux de données et des véhicules,

- Les changements fréquents de topologie et les mouvements rapides des véhicules.

Une des caractéristiques principales du réseau SDN est de découper le système de réseau en plan de contrôle et en plan de données :

- **Le plan de contrôle** : Centre de contrôle logique centralisé, il prend les décisions de transfert de paquets,
- L**e plan de données** : Il transmet les demandes au plan de contrôle et traite les décisions de transmission de paquets prises par le plan de contrôle.

C'est un système plus de programmable et flexible.
Le SDN propose trois façons de communiquer :

- **WIFI/DSRC** (dedicated short-range communication) : Entre deux véhicules ou bien un véhicule et une RSU (Road-Side Unit),
- **Liaison cellulaire** : Entre la station de base et le véhicule en dehors de la région DSRC,
- **Réseaux de fibres optiques câblés** : Parmi des unités de chantiers, les stations de base et les contrôleurs SDN.

E. Sécurité, anonymat et vie privée

1. Objectifs

Pour la sécurité des réseaux sans fils, il s'agit de garantir la confidentialité, l'intégrité et la disponibilité des service. Plus la connectivité est croissante, plus cette tâche sera difficile.

Il faut assurer la sécurité sur ces deux aspects :

- Seules les personnes autorisées peuvent accéder au réseau,
- Les services doivent être assurés correctement.

2. Caractéristiques de la sécurité dans VANET

Pour mieux comprendre les façons d'améliorer la sécurité dans les VANETs, il est nécessaire d'analyser la nature des communications et leurs caractéristiques :

- La communication sans fils possède un support de transmission partagé, elle permet d'agir en injectant des données erronées, ou des informations falsifiées dans le réseau.
- La communications sans fils est une communication à multi-sauts : les VANETs ont besoin d'une communication sans fil sur une très grande portée afin d'atteindre certaines entités du réseau. Pour cette raison, il est nécessaire d'utiliser des communications multi-sauts (pour atteindre une destination, un nœud peut utiliser d'autres nœuds en tant que relais). Mais certains **entité malveillantes** exploitent cette caractéristique pour mettre en péril le réseau.
- Dans certains protocoles des réseaux VANET, il y a le problème de la diffusion d'information de localisation. Les entités envoient périodiquement des messages qui indiquent leurs localisations. Des entité malveillante peuvent alors facilement poursuivre les entités qui les intéressent (**vols d'identités**)
- Les opérations sont autonomes. Les **entités malveillantes** peuvent envoyer des informations erronées ou falsifiées pour causer le dysfonctionnement du système.

3. Exigences pour une application ou un protocole de sécurité dans le réseaux VANETs

Ces exigences sont :

- **L'intégrité** : Il s'agit du service qui détecte la falsification des entités non autorisées. L'authentification des messages permet d'assurer que les données reçues n'ont subi aucune altération, modification ou duplication.
- **La non-répudiation** : Permet d'identifier chaque entité qui diffuse un message sur le réseau).
- **La confidentialité** : Permet de préserver le secret des véhicules et de fournir l'anonymat aux expéditeurs des messages échangés dans le réseau.
- **la disponibilité** : Pour garantir que toutes les ressources et services prévus sur le réseau sont disponible à tout moment avec un accès rapide et fiable aux informations importantes. Elle nécessité des protocoles de sécurités de très haute performance.

4. Le cas des réseaux sans fil basé sur la confiance et la réputation

Grâce au DSRC, les VANETs ont pu établir des connexions entre les différents véhicules changeant de direction fréquemment. Les véhicules communiquent directement avec les autres véhicules et envoient des informations à des infrastructures fixes sur le bord des routes. Dans la sécurité, l'approche traditionnelle est basée sur des outils et mécanismes de chiffrement. Cependant cette approche ne permet plus d'assurer la défense contre des nouveaux types d'attaques et de comportements. Les réseaux basés sur la réputation et la confiance où les différents nœuds maintiennent un niveau de notoriété auprès des autres et l'utilisent afin d'évaluer la fiabilité des messages envoyés sont déployés pour apporter des solutions aux comportements malveillants de certains nœuds, notamment dans le cadre des VANETs.
La sécurité dans les VANETs est d'autant plus importante qu'elle impacte directement la vie des passagers. Cependant, l'architecture décentralisée dans des topologies dynamiques complexifie cette tâche. Les modèles de confiance sont basés sur la vérification des véhicules et affectent une valeur de confiance à chacun d'entre eux. Ce taux de confiance peut provenir d'autres véhicules également. C'est donc en classant les nœuds par niveau de confiance qu'on va pouvoir établir sécuriser les différents réseaux.

Les VANETs étant des réseaux ouverts, n'importe quel véhicules peut venir l'intégrer ou le quitter à tout moment et aucun mécanisme n'est présent pour permettre à des véhicules de se reconnaître dans une prochaine communication. Ces différentes topologies, la rapidité du trafic et son imprévisibilité ont mené à diverse méthode d'affectation de confiance :

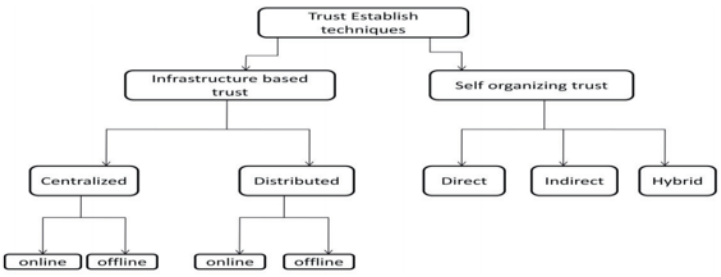


Fig. 3. Trust establishment models [34]

Confiance basé sur l'infrastructure

Concernant les méthodes de confiance basées sur les infrastructures, elle repose principalement sur des paramètres systèmes bien connus de tous et de confiance qui peuvent être utilisés lors des messages d'authentifications.

Certificats

Il s'agit surement de la plus populaire et la plus répandue des méthodes de confiance : le standards X.509. Ce certificat contient des attributs tels que :

- Le nom,
- Le rôle,
- Une clé publique,
- Une période de validité.

Comme on relie un nom à une clé, il s'agit d'un certificat d'identité et un vérificateur peut facilement certifié que le nom prétendu correspond bien avec celui du certificat qui a été transmis par une autorité de confiance. Dans cette configuration, l'unicité des nom est alors nécessaire : ils sont définis de manière hiérarchique dans la norme X.500. Dans la norme X.509, des champs additionnels peuvent être insérer dans ces certificats. De cette manière, les différents nœuds peuvent vérifier la valeur des informations transmises par le biais de celui-ci. Ce mécanisme est connu sous le nom de **SDSI (Simple Distributed Security Infrastructure)**.

Le **SPKI (Simple Public Key Infrastructure)** est un autre exemple basé sur les certificats. Dans ce modèle, on se sert uniquement de la clé publique des différents nœuds. Une notion de délégation est ajoutée permettant à un nœud de transmettre ou non l'information en fonction des droits associés : on a alors construit des chaînes de certificats vérifiables.

En 1997, une combinaison des deux méthodes est créé basé sur des identifiants : **Trust Management Systems** dans laquelle il est possible de rajouter des règles de sécurité, par exemple des restrictions d'IP.

Pour les VANETs, cela est particulièrement utile dans des environnements très dynamiques où les nœuds ne se sont quasiment jamais croisés. Cependant, cela relève des problèmes de protection de la vie privée, les certificats sont liés individuellement aux nœuds et peuvent en permettre l'identification. De plus, la vérification des certifications doit être un mécanisme très rapide au vu des contraintes temporelle des VANETs.

Kerberos

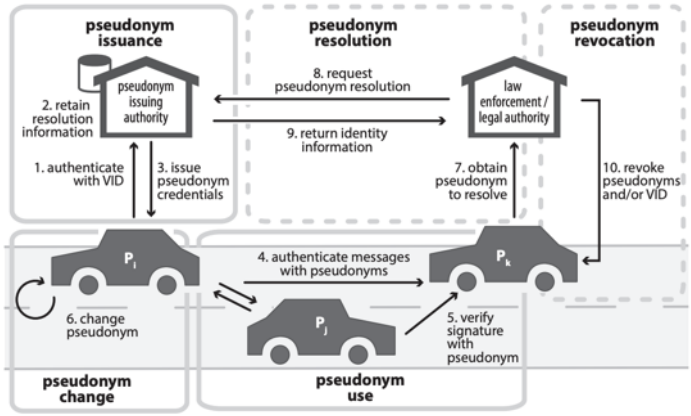
Cette méthode se base sur un système d'interaction en ligne avec un "Key Distribution Center" (KDC) qui se charge de l'authentification afin de valider un token de confiance pour un service donné.
Ce token contient :

- Un numéro de session,
- Une durée de validité (pour pallier aux attaques répétitives),
- La clé du nœud source chiffrée par la clé secrète du serveur.

Les informations de connexion sont conservées localement. Pour chaque nouvelle connexion, une procédure de certification en ligne avec une validation centralisée doit être lancée. La vie privée est désormais plus sécurisée par le chiffrement, mais cela reste très dépensier en temps.

Pseudonyms

Les méthodes énoncées révèlent l'identité des noeuds, soit par le biais de nom ou de clé, mais les réseaux véhiculaires demandent un niveau de sécurité très important. C'est dans cette optique que les pseudonymes entrent en jeux : ils changent au cours du temps et peuvent être modifiés par l'utilisateur lui-même. Il ne s'agit pas d'un anonymat complet mais ils confèrent tout de même une forte sécurité. Dans ces conditions, l'autorité centrale est la seule entité du système de confiance qui peut résoudre l'association des pseudonymes et de l'identité réelle des véhicules. Dans cette optique, les méthodes sur les certificats pourraient être améliorées avec l'utilisation de pseudonymes afin de palier au problème d'anonymat.



Blind signature

D'autres systèmes vont plus loin avec la mise en place de signatures aveugles (= certificats anonymes) qui permettent la signature d'un contenu sans le connaitre. Concrètement :

1) Un noeud qui demande un certificat, créé N certificats aveugles avec N pseudonymes différents.
2) Lors d'une demande d'authentification, l'autorité centrale demande alors d'en supprimer N-1 aléatoirement.
3) Dans le cas où celui restant est conforme syntaxiquement, l'autorité le signe sans connaître le pseudonyme associé et garantit ainsi l'anonymat du nœud.

De plus, l'autorité de confiance garde en mémoire les demandes et évite ainsi les attaques d'Overflooding. Ce mécanisme reste compatible aux approches par certificats et pseudonymes en garantissant l'anonymat.

Non-Interactive Zero-knowledge proof (NIZKP)

Les approches zéro-connaissances peuvent également être utilisées pour l'établissement de l'anonymat. Un nœud peut prouver la vérité d'une assertion (son certificat) a un vérificateur sans pour autant le révéler. Ils s'échangent des informations et le vérificateur vérifie si la réponse finale est positive (cela est schématisé par des défis/réponses). Ces défis sont basés sur des chaînes de caractères.
Les besoins d'une forte interaction entres les nœuds ont été dépassés par NIZKP en intégrant des interactions unidirectionnels : du demandeur vers le vérificateur.

Digital credentials

Les identifiants digitaux combinent l'approche des signatures aveugles et des approches zéro-connaissance.
Ainsi les noeuds détiennent des certificats pouvant divulguer des informations et en cacher d'autres à leur convenance. Les attributs sont compris au sein des clés publiques et privées de chaque noeud afin que les vérifieurs puissent avoir accès à certains attributs et authentifier la communication sans pour autant tous les connaître. La clé secrète du demandeur reste alors inconnue.

Group signatures

Cette méthode est basée sur le concept suivant : une clé publique possède un grand nombre de clé privée associée. Chaque membre du groupe se voit remettre un certificat privée qui peut ensuite être utilisé pour générer des signatures associés à la clé publique correspondante. Un noeud extérieur peut seulement voir que la validation a été effectué par un membre du groupe sans pour autant connaître lequel. Dans ce type d'infrastructure, une entité centrale peut faire l'association entre la clé privée et un noeud.

Confiance autogérée

Dans un réseau basé sur la confiance qui ne bénéficie pas de paramètres globaux, d'autres mécanismes doivent se mettre en place. Dans un VANET, il est possible de ne pas être connecté avec des infrastructures. Cependant, on doit toujours être en mesure d'analyser les données collectées de noeuds inconnus. Les réseaux de confiance autogérés possèdent deux caractéristiques :

- Il n'existe pas de tiers de confiance,
- Il n'existe pas d'informations globales partagées entre les différents noeuds.

Cela implique une gestion dynamique de la confiance. Ce niveau de confiance dépend également du temps de connexion et de la portée à laquelle se trouve l'autre noeud. On distingue alors 3 types de mécanismes de confiance :

- **Direct** : La confiance provient d'un échange mutuel entre les noeuds.
- **Indirect** : Les noeuds échangent des informations et des niveaux de confiance entre eux (transitivité de la confiance).
- **Hybride** : Combinaison des mécanismes direct et indirect.

CONFIDANT

Le protocol CONFIDANT permet la détection et l'isolation de noeuds non coopératifs dans un MANET. Il agit comme une extension de protocole de routage. Il tire son fonctionnement d'une expérience sur le comportement social des oiseaux.
Il y a quatre entités avec des caractéristiques précises impliquées dans ce protocole :

- Le **moniteur** : Regroupe les informations du voisinage en observant le protocole de routage. Si un dysfonctionnement ou un comportement étrange se produit, le système de réputation est informé.
- Le **gestionnaire de confiance** : Alerte les noeuds "amis" sur le dysfonctionnement d'un noeud. Ces messages sont cryptés pour en garantir l'authenticité.
- Le **système de réputation** : Gère les valeurs de confiance affectées aux différents noeuds. Ces valeurs proviennent d'expériences propres, des informations du voisinage et des messages d'alerte. Lorsqu'une valeur descend en dessous d'un seuil, le gestionnaire de chemin est prévenu.
- Le **gestionnaire de chemin** : Isole un noeud malveillant pour garantir la fiabilité du réseau. Cela se traduit par un routage autour de ce noeud et l'ignorance de ses messages.

Le protocole CONFIDANT permet une grande modularité dans la création du réseau de confiance. Cependant au sein d'un VANET, il reste difficile de différencier un comportement malveillant d'un changement de typologie rapide du réseau.

Location limited channels

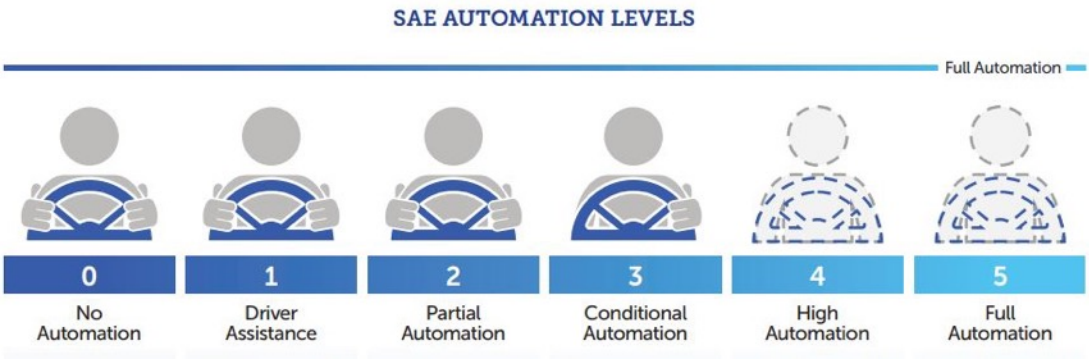
Les canaux de proximité peuvent également être utilisé pour l'établissement des relations de confiance au sein d'un réseau. Un réseau différent, séparé de celui de la communication principale est construit de telle manière qu'un attaquant ne peut pas y accéder directement. Ainsi, deux noeuds peuvent échanger des informations sensibles sur un canal sécurisé. Ces canaux sont principalement utilisés lors de l'authentification de deux noeuds dans les réseaux ad hoc dans lesquels ils échangent leur clé ou un hash de leur clé pour dialoguer par la suite. Le reste passe toujours par le réseau normal.

D'autres méthodes ont également été créées mais elles ne permettent pas être utilisées dans un milieu de contrainte tel que celui d'un VANET. Ce tableau résume les points positifs et négatifs des différentes méthodes ainsi que leur applicabilité. On constate ainsi qu'aucune de ces méthodes ne parvient à répondre parfaitement aux contraintes des VANETs. Il est alors envisageable de combiner les méthodes en fonction des situations pour essayer de tout prendre en compte.

	no online infrastr.	dynamic	privacy	timelin.	applicab.
Certificates	+	0	−	0	+
Kerberos	−	0	+	−	+
Pseudonyms	+	0	0	0	+
Blind Sign.	+	0	0	0	+
ZKP	+	0	+	−	+
NIZKP	+	0	+	0	+
Dig. Cred.	+	0	0	0	+
Group Sign.	+	0	+	0	+
Thresh. Cryp.	+	−	0	0	−
CONFIDANT	+	+	0	−	+
Nuglets	+	+	+	0	−
SPRITE	+	+	0	0	−
LLSC	+	+	0	+	+

F. Les voitures autonomes

On peut définir plusieurs niveaux d'autonomie pour une voiture (Classification de la SAE ou Society of Automotive Engineers):



- **Niveau 0 :** Le système automatisé émet des avertissements et peut momentanément intervenir mais n'a pas de contrôle permanent sur le véhicule.

- **Niveau 1 ("Mains sur le volant") :** Le conducteur et le système automatisé partagent le contrôle du véhicule.
  Exemples :
  Le régulateur de vitesse adaptatif (AAC) où le conducteur contrôle la direction et le système automatisé contrôle la vitesse.
  L'assistance au stationnement, où la direction est automatisée alors que la vitesse est contrôlée manuellement. Le conducteur doit être prêt à reprendre le contrôle total à tout moment.
  Le maintien de la voie (LKA) de type II est un autre exemple de conduite autonome de niveau 1.

- **Niveau 2 ("Mains libres") :** Le système automatisé prend le contrôle total du véhicule (accélération, freinage et direction). Le conducteur doit surveiller la conduite et être prêt à intervenir immédiatement à tout moment si le système automatisé ne répond pas correctement. Le terme "mains libres" ne doit pas être pris à la lettre. En fait, le contact main-volant est souvent obligatoire en conduite SAE 2 pour confirmer que le conducteur est prêt à intervenir.

- **Niveau 3 ("yeux libres") :** Le conducteur peut en toute sécurité détourner son attention des tâches de conduite. Par exemple, le conducteur peut envoyer un SMS ou regarder un film. Le véhicule gérera les situations qui appellent une réponse immédiate, comme le freinage d'urgence. Le conducteur doit toujours être prêt à intervenir dans un délai limité, spécifié par le fabricant, lorsque le véhicule le lui demande. L'Audi A8 Luxury Sedan 2018 a été la première voiture commerciale à prétendre être capable de conduire de manière autonome au niveau 3. Cette voiture aurait un pilote d'embouteillage. Lorsqu'il est activé par le conducteur, le véhicule prend le contrôle intégral de tous les aspects de la conduite dans des conditions de circulation lente jusqu'à 60 km / h. La fonction n'est valable que sur les autoroutes avec une barrière physique séparant un flux de voitures venant en sens inverse.

- **Niveau 4 ("cerveau libre") :** Comme pour le niveau 3, aucune attention du conducteur n'est nécessaire pour que la conduite se fasse en sécurité. Par exemple, le conducteur peut dormir en toute sécurité ou quitter son siège. L'auto-conduite n'est prise en charge que dans des zones spatiales limitées (geofenced) ou dans des circonstances particulières, comme des

embouteillages. En dehors de ces zones ou circonstances, le véhicule doit pouvoir interrompre le voyage en toute sécurité, par exemple garer la voiture si le conducteur ne reprend pas le contrôle.

- **Niveau 5 ("volant optionnel") :** Aucune intervention humaine n'est requise. Un exemple pour ce niveau serait un taxi robotisé.

Ces différents niveaux d'automatisation de la conduite nous permettent de prendre conscience que, sous certaines conditions, des voitures déjà commercialisée sont capables d'un certains niveau d'autonomie (niveau 3 pour l'Audi A8 Luxury Sedan par exemple).

Cependant, ce degré d'autonomie a été atteint sans avoir besoin de "connecter" la voiture à un réseau. Pour l'Audi A8, c'est le système intégré LIDAR qui permet cette autonomie grâce à des radars à courte et longue portée, des caméras et une batterie de capteurs. Sa "conduite autonome" est connue sous l'appellation "AI traffic jam". Dès qu'un embouteillage se forme sur l'autoroute et que les voies sont séparées par un terre-plein, le conducteur a la possibilité de déclencher la fonction en appuyant sur le bouton "AI". Le contrôleur central d'assistance à la conduite (zFAS) (composé de puces NVIDIA Tegra K1) prend alors la main.

Même si, en théorie, ce véhicule est capable d'un degré d'autonomie permettant au conducteur de lâcher le volant, cet acte est encore formellement interdit en France. Par ailleurs en France, seul 2 000 km de route sont ouvert aux tests de véhicules autonomes et ce depuis 2015.

Puisque cette avancé a été possible uniquement grâce à des capteurs, on peut se demander qu'est-ce qu'un réseau pourrait apporter aux véhicules autonomes ?

Qu'est-ce qu'une connectivité au réseau pourrait améliorer ?

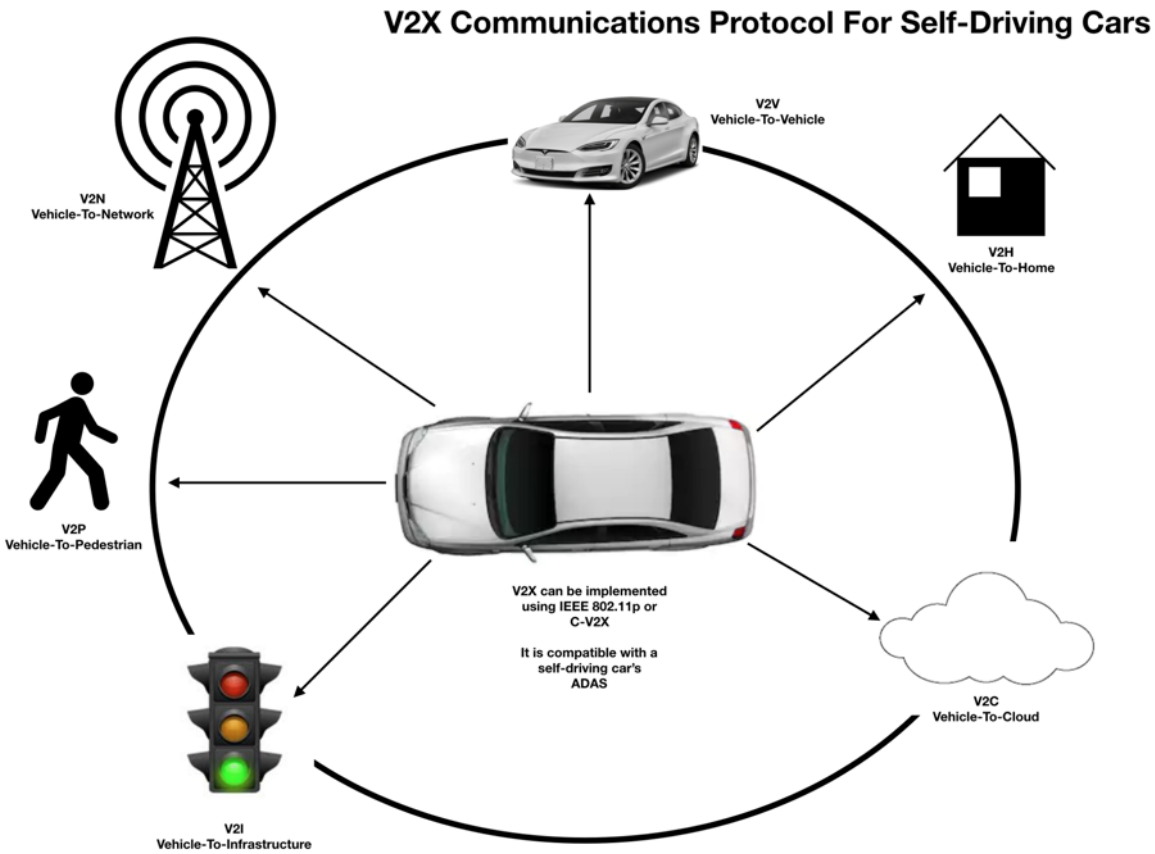
Pour répondre à cette problématique, un protocole V2X ou Vehicule-to-Everything serait une incroyable avancée. Pour l'instant, l'intelligence artificielle utilisant des techniques de machine learning a été la dernière avancée en terme de logiciel pour véhicules autonomes.

Une couche de protocole de communications pour les voitures autonomes peut apporter de nouvelles améliorations pour la conformité au niveau 5 de la norme SAE. Ce protocole prendrait en charge les communications :

- V2V (véhicule à véhicule) : Permettant aux voitures autonomes équipées de la technologie V2X de communiquer entre elles.
- V2I (véhicule à infrastructure) : Permettant aux voitures autonomes d'obtenir des informations sur les bâtiments, les ponts, les routes, les feux de circulation, etc …
- V2P (véhicule à piéton) : Utilisant des systèmes de détection de piétons pouvant fonctionner avec le système ADAS* d'une voiture,
- V2H (véhicule à domicile) : Les maisons intelligentes pouvant envoyer et recevoir des informations directement à partir de la voiture,
- V2N (véhicule à réseau) : Connexion mobile entre la voiture et le réseau cellulaire d'un opérateur,

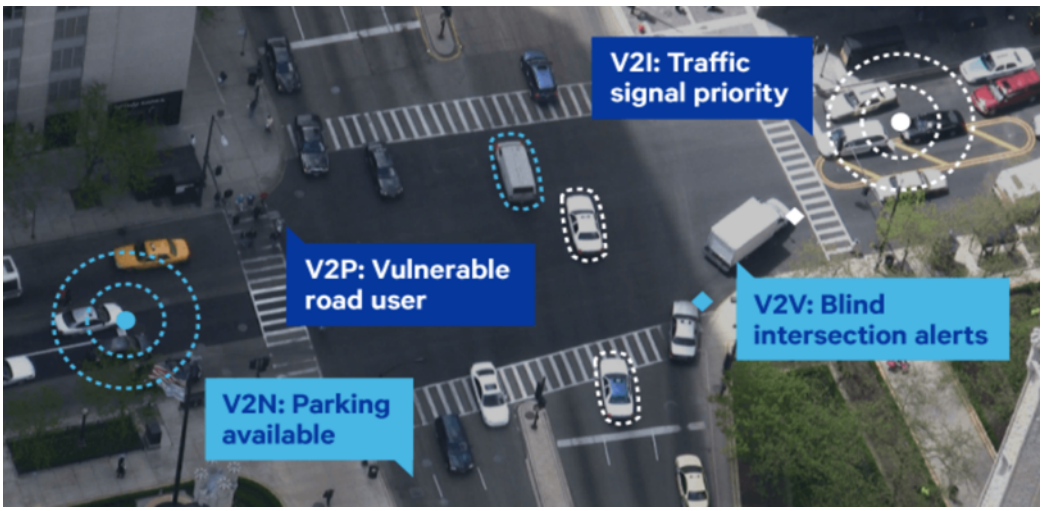
- V2C (véhicule à Cloud) : Fournissant un accès direct aux réseaux cloud à l'aide de connexions TCP / IP sécurisées.

* ADAS (Advanced Driver Assistance Systems) : Ensemble de dispositifs permettant d'assurer tout ou partie des tâches de conduite avec un niveau d'automatisation entre 2 et 4 (selon la classification SAE).



Cela permettrait aux voitures autonomes de communiquer et de partager des informations entre elles. Cela rendra également les voitures autonomes plus sensibles les unes aux autres à la manière dont les gens interagissent. Enfin, cela permettrait la communication directe avec des infrastructures telles que des bâtiments intelligents, des routes intelligentes, des feux de circulation, des ponts, des voies ferrées, des aéroports et d'autres systèmes de transport intelligents.

Cette technologie utiliserait des signaux sans fil à courte portée pour communiquer à l'aide d'un réseau conforme à leurs normes. Cela pourrait résoudre de nombreux problèmes auxquels sont confrontés les développeurs de voitures autonomes pour assurer la sécurité de l'utilisation de véhicules autonomes à usage commercial et sans conducteur. V2X est destiné à être implémenté et déployé de manière décentralisé sans aucune autorité unique contrôlant les voitures. Chaque voiture autonome aura son propre système de capteur V2X indépendant, de sorte qu'elle n'a pas besoin d'un opérateur central. Les capteurs conçus pour prendre en charge V2X sont à bande passante élevée, à faible temps de latence et prennent en charge des liaisons à haute fiabilité. Ces capteurs sont également conçus pour fonctionner par mauvais temps, offrant une fiabilité accrue en cas de besoin.



Ce protocole V2X aurait 3 objectifs principaux :

- **La Sécurité routière** : Afin de garantir la sécurité routière, V2X doit pouvoir améliorer la sécurité globale. Cela inclut (entre autres) le freinage automatique d'urgence AEB, la détection de collision, les avertissements de danger de la route, l'avertisseur d'angle mort et la formation de pelotons ou la création de distances de sécurité pour les véhicules autonomes sur les routes et les autoroutes. Le déploiement des AHS (Automated Highway Systems), également appelé «routes intelligentes», fournit un système de transport intelligent visant à prévenir et à éviter les accidents grâce à un système de communication coordonné. Par exemple, la voiture A évitera de heurter la voiture B sur la base d'une distance de sécurité mesurée sur la route. Il est encore plus important d'empêcher les voitures autonomes de heurter les piétons qui traversent la rue. Les informations provenant de la route ou de l'intersection peuvent donner à une voiture autonome équipée de la technologie V2X une visibilité sur les zones de passage piétons et même l'alerter lorsqu'un piéton traverse effectivement la rue. Cela peut fonctionner avec le système LiDAR ou le système de vision d'une voiture autonome.

- **Amélioration de la circulation** : L'utilisation de la reconnaissance et de l'évitement de la congestion permettra aux voitures autonomes de comprendre les conditions de la route. Bien que cela soit censé rendre les voitures autonomes plus conscientes du trafic, cela dépendra beaucoup de la ville et de la qualité de la cartographie de la région. L'idée ici est que les voitures autonomes peuvent partager des informations entre elles sur les conditions de circulation dans leur région. L'utilisation de systèmes de navigation peut être interfacée avec la voiture autonome par le biais d'une API. Les systèmes de navigation peuvent alors utiliser un algorithme pour calculer des itinéraires afin d'éviter les routes encombrées. Parmi les autres informations pouvant être partagées figurent la présence de barrages routiers, de fermetures d'intersections,

d’accidents et d’autres informations relatives à la route. Une autre application de ce système est la navigation intelligente dans laquelle les voitures autonomes peuvent explorer le meilleur itinéraire vers une destination dans les plus brefs délais.

- **Économies d'énergie** : L’énergie peut être économisée lorsque les voitures autonomes suivent des itinéraires optimaux.

Actuellement, le système ADAS (système d'assistance au conducteur évolué) de certaines voitures, comme le pilote automatique amélioré Tesla, modèle S, offre des fonctionnalités semi-autonomes. Ce que V2X peut faire, c'est utiliser les fonctionnalités du logiciel ADAS pour offrir davantage de fonctionnalités. Par exemple, le V2X peut fournir des informations au système AEB de la voiture pour donner des informations plus précises sur le moment opportun pour freiner en cas d’urgence. Un autre exemple est d’améliorer la fonctionnalité de changement automatique de voie en vérifiant que la voie est parfaitement dégagée et sûre.

Deux solutions techniques sont envisageables pour implémenter ce système :

- Une architecture basée sur le WLAN utilisant la norme sans fil IEEE 802.11p DSRC,
- LTE à base cellulaire appelé «Cellular V2X» ou C-V2X qui utilise les réseaux 4G et 5G.

Dans une étude de 2017, C-V2X utilisant LTE s'est révélé supérieur à la norme 802.11p en terme de performance, de portée de communication et de fiabilité. Les deux normes pourraient très bien fusionner pour offrir les meilleures fonctionnalités des deux systèmes.

V2X peut être implémenté de deux manières. La FCC a attribué un spectre de 75 MHz dans la bande de 5,9 GHz aux systèmes de transport intelligents (STI). L'une des méthodes utilisées par V2X consiste à utiliser les communications DSRC (Dedicated Short Range Communications) dans la spécification IEEE 802.11p. L'autre façon est de passer par C-V2X ou Cellular V2X. C-V2X qui utilise les réseaux LTE 4G existants pour communiquer, et s'étendra à la 5G lorsqu’elle sera disponible.

6. Conclusion et Perspectives

En conclusion, nous pouvons dire que les réseaux véhiculaires sont encore en cours de développement.

Dans une première partie, nous avons distingué les objectifs principaux de ces réseau et identifié les normes européennes et mondiales qui doivent régir leur utilisation.

Dans un deuxième temps, nous avons détaillé les applications diverses et ambitieuses de ces réseaux.

Nous avons ensuite comparer les différentes technologies sur lesquelles ces réseaux pourraient reposer. Cette partie a également fait l'objet d'une étude approfondie sur la 5G, technologie d'avenir incontournable pour les réseaux véhiculaire.

Enfin, nous avons dédié une partie aux challenges apportés par les réseaux véhiculaires et expliquer certaines solutions déjà apportées (routage, priorisation et congestion, formation de clusters, sécurité). Cette partie s'est conclue sur une perspective d'évolution appliquée aux voitures autonomes qui reprend les concepts détaillé dans le rapport en proposant une solution innovante et réaliste : la V2X.

Bibliographie

- A Survey on Software-defined Vehicular Networks, 2017
- Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions, 2011
- Vehicule en reseau UTC
- Vehicular Ad Hoc Networks (VANET): Architectures, methodologies and design issu
- Intelligent Vehicular Networks and Communications : Fundamentals, Architectures and Solutions - Anand PAUL, Naveen CHILAMKURTI, Alfred DANIEL, Seungmin RHO - Edition ELVESIER
- Thèses de doctorants de l'UTC :
    - Thèse de Farah EL ALI - Communication unicast dans les réseaux mobiles dynamiques - 2012
    - Thèse de Sofiane KHALFALLAH - Algorithme best-effort pour les réseaux dynamiques - 2010
    - Thèse de Mohamed Oussama CHERIF - Optimization of V2V and V2I communications in an operated vehicular network
- http://www.ijarcs.info/index.php/Ijarcs/article/viewFile/2735/2723
- https://www.researchgate.net/figure/VANET-Architecture_fig1_280958696
- http://journals.sagepub.com/doi/full/10.1155/2015/745303
- https://hal.inria.fr/inria-00419466/document
- Traité Réseaux et Télécoms "Réseaux Véhiculaires : modèles et algorithmes", H. LABIOD et A-L BEYLOT, Ed. Lavoisier.
- http://www.iro.umontreal.ca/~echo/Conference/2014/Reseaux-vehiculaires-DIRO-Hafid-10-15-14-public.pdf
- https://www.iso.org/committee/54706.html
- http://user.it.uu.se/~erikn/files/DK2-adhoc.pdf
- https://hal.archives-ouvertes.fr/hal-00781267/document : Hiérarchisation dans les réseaux ad hoc de véhicules, 2012
- https://journals.sagepub.com/doi/pdf/10.1155/2015/745303 : Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends, 2014
- https://www.hds.utc.fr/~ducourth/dokuwiki/_media/fr/t-tutorial-vanet-jnctt2011-bducourthial.pdf
- http://www.rfwireless-world.com/Tutorials/802-11p-WAVE-tutorial.html
- https://www.standards.its.dot.gov/Factsheets/Factsheet/80
- A Survey on Vehicle to Infrastructure Communication System, Ms. Bharati Punjabi
- Performance Evaluation of IEEE 1609 WAVE and IEEE 802.11p for Vehicular Communications
- https://ac.els-cdn.com/S1874490715000531/1-s2.0-S1874490715000531-main.pdf?_tid=2b0ec666-e5bd-4555-82bf-8c7ccbf42ef1&acdnat=1544049680_6f780c97ceb845e9a247e42e5be0d2c3 , A survey on 5G: The next generation of mobile communication
- 5G Next generation VANETs using SDN and Fog Computing Framework

- Securite et reseaux de confiance :
    - A Survey on Reputation and Trust-Based Systems for Wireless Communication Networks
    - Trust based approaches for secure routing in VANET: A Survey
    - Trust Issues for Vehicular Ad Hoc Networks
- Véhicules autonomes :
    - https://www.inria.fr/en/content/download/110728/1845174/version/2/file/InriaLivre+blanc_VAC.pdf
    - https://medium.com/self-driving-cars/improving-self-driving-car-safety-and-reliability-with-v2x-protocols-1408082bae54
    - https://www.researchgate.net/publication/221450143_V2X-Based_Traffic_Congestion_Recognition_and_Avoidance
    - https://www.zdnet.com/article/what-is-v2x-communication-creating-connectivity-for-the-autonomous-car-era/
    - https://www.qualcomm.com/media/documents/files/accelerating-c-v2x-commercialization.pdf