QoS, PERFORMANCES, SECURITE ET DES COMMUNICATIONS DANS L'IoV

Lylia Alouache, Rachid Chelouah, Nga Nguyen

lylia.alouache, rachid.chelouah, nga.nguyen [@eisti.eu]

ABSTRACT :

La nouvelle ère de l'Internet des Objets (IoT : Internet of Things) a suscité l'évolution des réseaux ad hoc véhiculaires classiques (VANET) vers le paradigme de l'Internet des véhicules (IOV : Internet of Vehicles).Dans cette partie émergente de l'IoT, les objets sont des véhicules intelligents interconnectés, qui accèdent au réseau internet pour l'échange et le traitement des données. Ils utilisent des communications V2Vn(véhicule à véhicule), V2R(véhicule à route), V2H (véhicule à humain), V2S (véhicule à capteur externe), ce qui forme alors un système de communication mobile et dynamique.

Aujourd'hui les vehicules qui sont capable d'atteindre de grande vitesses, et traverser de longues distances en un minimum de temps peuvent se retrouver bloqués pendant des heures à cause des embouteillages (entretiens routier / accidents ou autre). Une quantité significative d'accidents sont provoqués par la fatigue du conducteur, le manque d'alerte rapide sur les conditions de la route, ou le manque d'entretien des véhicules.

Nos véhicules sont aujourd'hui équipés d'ordinateurs de bord et de capteurs sans fil capables de recueillir et de traiter une grande quantité de données internes comme la vitesse, la pression sur les pédales, l'angle du volant, les signes de fatigue et de somnolence du conducteur, l'emplacement géographique (GPS), ou des information sur l'environnement extérieurs, l'état des routes, les incidents sur les routes ou simplement pour rendre un trajet agréable.

L'IoV permet donc l'acquisition et le traitement de grandes quantités de données provenant de zones géographiques polyvalentes via les plates-formes intelligentes des véhicules. Il offre diverses catégories de services relatives à la sécurité routière aux conducteurs et au confort des passagers. Remédier à ces contraintes du quotidien constitue le défi majeur de l'IoV.

Notons que l'IoV est étroitement lié à l'environnement cloud computing car il permet de mettre en pratique ce concept pour les systèmes de transport intelligents.

Il existe de nombreux défis, à relever dans l'IoV. Un des défis typiques est le grand volume de données à traiter et à stocker, ce volume est engendré par la quantité de capteurs et de véhicules présent sur les routes, Une autre problématique est d'assurer la sureté de fonctionnement des systèmes communicants et bien d'autres. Dans le cadre de cette présentation, on s'intéresse à la question des communications tolérantes aux perturbations de la connectivité, ce qui est critique pour les applications interactives à bord d'un véhicule. En effet, certains véhicules peuvent se trouver isolés sans possibilité d'émission ni de réception durant un laps de temps indéterminé.

La problématique consiste à étudier la disponibilité, la fiabilité et la robustesse des communications entres les agents de l'IoV. La nature dynamique de l'internet des véhicules présente des contraintes de communications à savoir des déconnexions fréquentes susceptibles d'être un obstacle pour les exécutions d'applications à bord d'un véhicule. En effet, certains véhicules se retrouvent parfois isolés sans possibilité d'émission et réception durant une période de temps indéterminée. Cette situation nuit à la qualité de service offert par l'IoV et par conséquent à son utilité. Certains obstacles peuvent engendrer des déconnexions dans l'IoV comme :

- la Forte mobilité des véhicules et le changement rapide de la topologie du réseau,
- la faible densité de véhicules sur les zones urbaines et autoroutes, et l'absence de bornes RSU,
- l'utilisation des réseaux cellulaires à couverture restreinte pour les communications,
- les attaques de type « Black Hole » et « Denis de service » que peut subir le réseau de communication,
- la surcharge du réseau due à la quantité d'agents communicants dans l'IoV, et la bande passante limitée,
- l'architecture distribuée et l'accès à distance aux services offert par l'IoV,
- l'hétérogénéité des entités qui constituent l'IoV,
- le manque de coopération entre les agents de l'IoV et certaines infrastructures qui peuvent être des relais de communication (à cause de différents niveau de sécurité par exemple),
- la complexité et la densité de l'environnement extérieur (forêt, building etc).

L'objectif consiste à fournir aux conducteurs et aux passagers l'accès continu et exceptionnellement à jour à des données opérationnelles, fraiches, disponibles et fiables, répondre ainsi aux besoins sans cesse croissant en termes de qualité de service et de sécurité dans l'environnement IoV. Il s'agit principalement d'améliorer des solutions existantes au niveau des couches réseau et application pour le support des règles QoS et de routage sécurisé. La solution au problème permet d'assurer la disponibilité des services et la fiabilité des données et la robustesse de l'IoV.

Le travail à réaliser consisterait en :

- Un état de l'état de l'art en matière de IoV et VANETs.
- Une étude des obstacles liés aux transmissions et exécutions des applications.
- Une étude sur la sécurité des communications dans l'IoV plus précisément sur les attaques par dénis de services qui affecte la qualité de service de l'IoV.
- Une étude sur le routage dans les réseaux véhiculaires.
- Une étude de quelques travaux concernant les attaques par dénis de service sur le réseau de communication des VANETS.
- Une proposition d'un mécanisme tolérant aux perturbations de connectivité.

L'idéale serait éventuellement de commuter entre les technologies de communications lorsqu'un problème survient, néanmoins elle présente beaucoup de contraintes (matérielles, juridiques ou autres).

On s'intéresse alors à la partie software où il s'agit principalement d'apporter des techniques efficaces, fiables, robustes et optimisées pour la transmission sécurisée de paquets de données en fonction de l'évolution de la topologie et de la mobilité du réseau. On essaye d'apporter des améliorations aux solutions existantes au niveau des couches réseau et application pour le support des règles QoS et de routage sécurisé pour un accès continu aux services.

Proposition : détection des zones noires et le moyen de les contourner dans les communications IoV

On considère ici un système de communication entre les agents mobiles de l'internet des véhicules.

L'objectif est d'offrir une connectivité sans interruption aux véhicules, conducteurs et passagers

On considère une zone bien déterminée, la proposition se décompose en cinq phases :

Phase 1 : estimation de la durée de contact entre les entités de l'IoV

Soit V un véhicule de l'IoV et V_i i Є N l'ensemble des véhicules voisins de V à un instant t.

Grace aux messages périodiques 'BEACON <x, y, v, $\overrightarrow{dir}$, id>', on estime les durées de contact entre chaque couple d'agents à l'instant t et t + dt. Les variables x, y représentent les coordonnées géographiques de l'agent mobile, V est la vitesse de déplacement, le vecteur $\overrightarrow{dir}$ donne le sens de déplacement, id est l'identifiant de l'agent.

Phase 2

Créer un fichier de log global, qui sera accessible en lecture et écriture par chaque agent de l'IoV. Lorsqu'un agent rencontre une anomalie ou subit une déconnexion, ce dernier met à jour le fichier log, avec tous les détails concernant cette anomalie, la durée de la déconnexion, la zone non couverte, la densité de véhicules dans cette zone, éventuellement la cause de la déconnexion, etc. Cette phase permet de détecter les zones noires, supprimer ce tronçon de toutes les tables de routage de l'IoV.

Phase 3

A un niveau plus bas du standard de communication, la couche réseau nous permettra de faire un mixe entre un routage réactif lors des communications sans anomalies, et basculer vers un routage prédictif en cas d'anomalies de communication (c'est-à-dire exploiter les routes alternatives pour l'acheminement des paquets qu'on obtient grâce à la phase 1).

Phase 4

Pour une meilleure efficacité de la proposition. Cette phase ordonnance les paquets de données à transmettre, lors de la phase de routage en fonction de deux paramètres :

a) l'information acheminée (un message d'urgence ou de l'info divertissement par exemple)
b) l'information de maintenance du système.

L'information de maintenance et de l'information intrinsèque destinée aux agents mobiles doivent être séparée. Cette phase permet d'exploiter et de profiter au mieux d'une connexion opportuniste qui s'offre à un agent mobile avant d'entrer dans une zone noire.
Ce qu'on essaye d'offrir également c'est une solution préventive, c'est-à-dire que l'on peut connaitre sa propre situation, c'est-à-dire qu'à l'instant t on a une probabilité P de se retrouver isolé du réseau de communication, et cela grâce au fichier log.
Dans le cas échéant, on profite de la communication actuelle pour privilégier et acheminer les informations destinées aux agents mobiles que celles de maintenance du système de communication en question.

Phase 5:

Elaborer une métrique qui mesure le taux d'indisponibilité de communication, et une métrique qui mesure le temps nécessaire au système pour contourner une zone noire.

L'objectif est de minimiser ces deux métriques par rapport à d'autres solutions existantes dans la littérature.