École Polytechnique Montréal

INF6909 : Projet d'études supérieures

SSVR

Philippe TROCLET 1815208

Soumis à : Mme. Bellaïche
Soumis le : 8 août 2016

Table des matières

1 Introduction

Depuis quelques années le sujet des objets connectés est très étudié. En effet, on leur prévoit un grand avenir, en plus d'améliorer l'expérience utilisateur au quotidien, ils permettraient d'améliorer la sécurité. Leur aspect connecté permettrait l'échange d'informations et donc de prévenir leur utiilisateurs d'un danger imminent.

Parmi ces objets on trouve les voitures connectées, ces dernières auraient certaines fonctionnalités destinées à améliorer le confort et la sécurité routière. Les exemples de telles fonctionnalités ne manquent pas, l'horizon des possibilités s'étend du simple mécanisme de messagerie à la gestion du traffic en passant par la formation de convois. (ces derniers permettraient une interaction entre les véhicules voire une automatisation de la conduite). Les applications possibles sont nombreuses et très étudiées [1, 2]. Mais, même si les possibilités sont immenses, il ne faut pas oublier qu'il existera toujours des individus mal intentionnées, des "attaquants", qui tenteront d'exploiter les vulnérabilités du système. Or dans le cas automobile, les dangers d'une telle attaque sont sans mesures avec ceux auxquels nous sommes habitués. Si un ordinateur est infecté, la victime subir un dommage financier ou moral, dans le meilleur cas un simple inconfort. Mais dans un contexte où la victime conduit un véhicule le moindre dysfonctionnent peut mener à un accident pouvant mener à la mort de la victime et des occupants des véhicules proches.

Ce problème est particulièrement présent dans les réseaux de véhicules ad-hoc où l'abscence d'une infrastructure centralisée rend difficile la vérification des informations ainsi que l'identification des véhicules malicieux. Pourtant ce type de réseaux est incontournable. Permettre l'accès un serveur central depuis toues les routes et autoroutes serait extrêment coûteux et prendrait un temps conséquent. Ainsi, une communocation ad-hoc permettrait, sous réserve qu'une certaine garantie de sécurité existe, permettrait aux utilisateurs de bénéficier de tous les avantages des voitures connectées à moindre coût, tant pour le particulier, que pour l'état (ou un quelconque autre organisme qui aurait à sa charge la gestion des routes). En effet, la seule condition pour qu'un tel réseau puuisse fonctionner est qu'une majorité des véhicules soient équipés des équipements nécessaires.

Aussi, même si sécuriser un réseau ad-hoc est un challenge, le potentiel retour sur investissement suffit à justifier l'effort. C'est ce constat qui a motivé la construction d'un système de réputation par R. Engoulou [3]. Système de réputation dont l'étude a été appronfondie par M. Mallis [4]. Nous allons donc travailler sur un modèle déjà existe afin d'améliorer ses performances ainsi que la qualité des résultats issus des simulations.

Le modème développé par nos prédécesseurs se base sur la création d'un système de réputation via une modification du protocole AODV. Le principe de ce système repose sur une modification de l'entête du dit protocole afin d'introduire des variables qui seront analysées par le système pour produire une note en fonction de laquelle la communication avec le noeud sera acceptée ou refusée.

1.1 Mise en contexte

Avant de présenter notre contribution, il convient de rappeler le fonctionnement du protocole AODV sur lequel se base les travaux SSVR (ou du moins la partie expérimentale). Cela nous permettra d'introduire le fonctionnement du SSVR, puis de présenter les enjeux et défis qu'un tel système rencontre dans le milieu des VANETs.

1.1.1 Le protocole AODV

Les détails du protocole AODV (Ad hoc On-Demand Distance Vector) sont disponibles dans la RFC 3561 [5]. Nous allons toutefois tenter de présenter les principales caractéristiques de ce protocole.

Ce dernier appartient à la catégorie des protocoles réactifs, c'est-à-dire qu'il va calculer une route perttant à un paquet d'atteindre un autre véhicule seuleemnt si la nécessité de communiquer avec ce véhicule se présente. De plus, ces routes ne sont maintenues que si elles sont utilisées. Cette spécificité du protocole permet de limiter la charge du réseau et donc d'améliorer ses performances.

AODV possède trois types principaux de messages :

- RREQ (Route Request) ce message permet d'initier la construction d'une route vers une nouvelle destination
- RREP (Route Respond) réponse à un message RREQ si on est la destination ou si l'on a une route vers la destination
- RERR (Route Error) erreur de routage, un lien est devenu invalide par exemple

Lors de la construction d'une route le noed émetteur envoie un message *RREQ* via un *broadcast* chaque noeud le recevant vérifie dans la table de routage s'il possède une route vers la destination si c'est le cas il répond via un *RREP* sinon il *broadcast* la requête à son tour. Lorsque chaque noeud ayant émis une *RREQ* reçoit une réponse il ajoute le noeud dont provient la réponse à sa table de routage et désormais il enverra chaque paquet devant être reçu par la destination à ce noeud qui sera chargé de l'envoyer au noeud qui lui avait répondu déclenchant ainsi lenvoie du *RREQ*. ce procédé continuera jusqu'à ce que le message atteigneale noued désigné. On soulignera que un message de demande de route est envoyé uniquement si le noued émetteur n'a pas de route ou si celle-ci n'est plus fonctionnelle.

Le protocole possède bien entendu d'autres subtilités, on pensera par exemple à l'utilisation de numéro de séquence pour éviter la formation de boucle ou encore à une optimisation basée sur le nombre de sauts pour obtenir des routes les plus courtes possibles, mais la connaissances de ces dernières n'est nécesaire pour la compréhension du SSVR.

1.1.2 Système de sécurisation des VANETs par Réputation

2 Conclusion

Références

[1] Richard Bishop. A survey of intelligent vehicule applications worldwide. 2000.

[2] Asim Rasheed, Haleemah Zia, Farhan Hashmi, Umair Hadi, Warda Naim, and Sana Ajma. Fleet & convoy management using vanet. 2013.

[3] Richard Gilles Engoulou. Sécurisation de vanets par la méthode de réputation des noeuds, 2013.

[4] Majid Mallis. Simulations et évaluation des performances du système de réputation pour les vanets, 2015.

[5] C. Perkins, E. Belding-Royer, and S. DAS. Ad hoc on-demand distance vector (aodv) routing. RFC 3561, july 2003.