Modèle décentralisé de Réputation basé sur le théorème de Bayes dans les réseaux véhiculaires

Maryam Najafi, Lyes Khoukhi, Marc Lemercier

Modèle décentralisé de Réputation basé sur le théorème de Bayes dans les réseaux véhiculaires

Maryam Najafi
Laboratoire Informatique et société numérique (LIST3N), Université de Technologie de Troyes (UTT), Troyes, France
Email: maryam.najafi@utt.fr

Lyes Khoukhi
Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France
Email: lyes.khoukhi@ensicaen.fr

Marc Lemercier
Laboratoire Informatique et société numérique (LIST3N), Université de Technologie de Troyes (UTT), Troyes, France
Email: marc.lemercier@utt.fr

***Abstract*—Le réseau ad hoc VANET est une technologie sans fil dédiée aux communications véhiculaires. Ces réseaux VANETs ne sont pas faibles et la sécurité doit être prise en compte comme l'un des problèmes les plus critiques. Pour renforcer la sécurité, nous proposons une méthode pour évaluer la confiance des communications véhiculaires et mesurer la fiabilité des véhicules. Nous présentons un modèle décentralisé de réputation dans lequel les nœuds représentent des véhicules. L'activité de chaque véhicule est observable par les nœuds adjacents. Notre modèle permet aux nœuds de détecter les véhicules malveillants et d'éviter d'interagir avec eux. Nous proposons d'utiliser un filtre Bayésien pour mesurer avec précision les scores de confiance des véhicules. Nous étudions également le concept de classification afin de distinguer le comportement des véhicules. Ensuite, nous analysons la précision de notre filtre bayésien en calculant les différents facteurs. Les simulations approfondies ont montré que le filtre proposé peut attribuer un score de confiance précis aux nœuds dans diverses configurations de réseau.**

I. Problématique et contexte

Le réseau VANET est un domaine de recherche prometteur offrant de nombreuses applications et services utiles. Il assure les communications entre les véhicules, ainsi qu'entre les véhicules et les équipements stationnaires [1]. La technologie VANET aiderait à prévenir les accidents, à améliorer le système de contrôle de la circulation et à rendre la conduite plus sûre et plus confortable. Les applications et services véhiculaires des VANETs sont déployés dans des environnements sans fil sans surveillance centralisée et quelques fois hostiles [2]. Les VANETs sont vulnérables à de nombreux types de menaces (par exemple modification des informations vitales) et la sécurité devient l'une des principales préoccupations [3]. Les messages modifiés par les attaquants peuvent inciter le réseau VANET à prendre de mauvaises décisions, ce qui peut entraîner des troubles dans la circulation et des accidents de la route. Dans la pratique, un véhicule doit vérifier la validité de tout message reçu avant de prendre des décisions. Certains travaux de recherche ne traitent pas suffisamment les problèmes suivants : 1) un comportement non coopératif des paquets non acheminés et 2) une génération non intentionnelle de faux messages [4].

Par conséquent, une approche de confiance robuste devrait tenir compte de diverses conditions de comportement et de situations incertaines.

II. Modèle Bayesian décentralisé de Réputation

Cet article présente un modèle décentralisé de réputation robuste basé sur le théorème de Bayes pour filtrer les véhicules malveillants dans les réseaux véhiculaires. Pendant le processus de surveillance, chaque nœud observe le comportement de ses voisins, en suivant l'approche de la méthode Watchdog. La topologie dynamique des réseaux véhiculaires exige que les algorithmes de gestion de la confiance soient capable de gérer des situations complexes et des données hétérogènes. Nous calculons la probabilité de comportement malveillant à l'aide du théorème Bayes. Nous utilisons le ratio de coût total (TCR) pour observer les performances du filtre proposé.

Notre modèle mesure le niveau de confiance et de fiabilité de chaque véhicule. Le score final du véhicule (FVS) mesuré est la combinaison des résultats du théorème de Bayes et de la méthode Watchdog. Un véhicule décide d'interagir ou non avec un autre véhicule en fonction de sa valeur de FVS. Ensuite, nous utilisons le modèle pour attribuer l'état possible pour chaque véhicule (normal "NO", légèrement suspect "LS", fortement suspect "HS", and malveillant "MA") avec l'identifiant v_{id}^t. Nous calculons le FVS du nœud avec la formule suivante :

$$FVS = \lambda * AVG(v_{id}^t, hv_s) + (1 - \lambda) * v_{id}^{t-1} \quad (1)$$

v_{id}^t représente le score de véhicule avec l'identifiant id à l'instant courant t, hv_s est la moyenne des opinions des voisins, et v_{id}^{t-1} est le score précédent du véhicule. En utilisant λ, la valeur de réputation récente a plus de poids que l'ancienne. Nous introduisons le concept de coût de classification erronée, qui est appelée β; chaque fois qu'une erreur de classification se produit, nous calculons le coût de transition c entre les états (MA, HS, LS, NO). Pour étudier la précision de notre filtre bayésien, nous calculons les facteurs Node Recall (NR) et Node Precision (NP) [5] :

$$NR = n_{MA \to MA}/N_{MA} \quad (2)$$

$$NP = n_{MA \to MA}/\Sigma n_{i \to MA} \quad (3)$$

Où $n_{x \to y}$ désigne le nombre de nœuds de classe x qui sont classés par erreur dans la classe y. N_i désigne le nombre total de véhicules avec l'état "i", $i = \{MA, HS, LS, NO\}$. Pour évaluer les performances du filtre, nous devons calculer à la fois la précision AC et l'erreur ($ER = 1 - AC$). Nous avons défini AC comme :

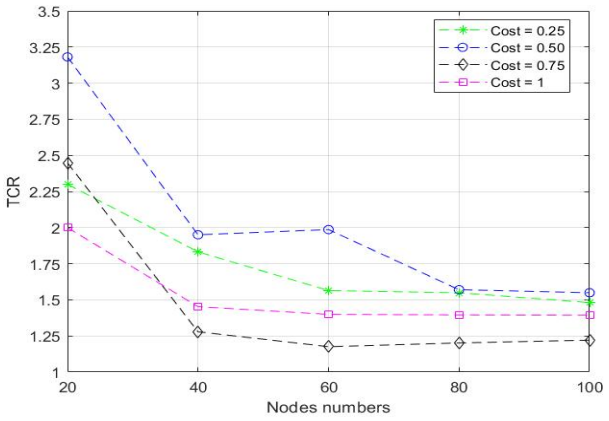

Fig. 1: TCR vs. évolutivité des nœuds (MA: 10%)

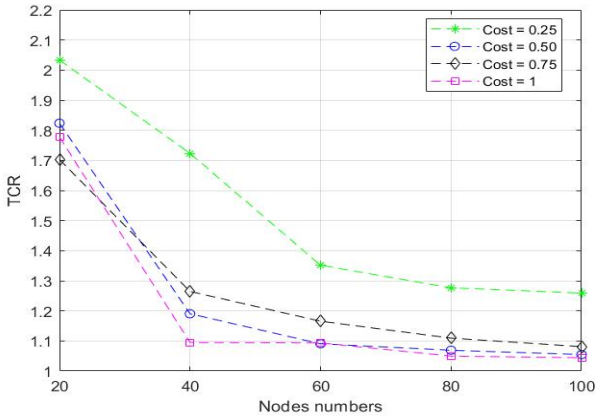

Fig. 2: TCR vs. évolutivité des nœuds (MA: 20%)

$$AC = \Sigma n_{i \to i} / (N_{MA} + N_{HS} + N_{LS} + N_{NO}) \quad (4)$$

Pour évaluer les performances de notre modèle proposé, nous avons effectué des simulations approfondies à l'aide de MATLAB. Nous calculons le ratio de coût total "TCR" pour analyser la précision de notre filtre bayésien, comme suit :

$$TCR = (C\_ER^*)/(C\_ER) \quad (5)$$

À partir de cette équation, nous concluons que si la valeur TCR est supérieure à 1, alors la classification est considérée comme acceptable. En effet dans ce cas, l'erreur de classification sans filtre C_ER^* doit être supérieure à l'erreur provoquée par le filtre C_ER.

Nous considérons un ensemble de réseaux composé de 20, 40, 60, 80, 100 véhicules. Nous avons consideré la proportion de nœuds malveillants à 10% et 20%. Ensuite, nous avons fait varier les valeurs du coût (c) d'une mauvaise classification, 0,25, 0,50, 0,75 et 1. Le but de ces scénarios de simulation est de trouver les meilleurs paramètres pour notre solution et d'évaluer la valeur du TCR en fonction du nombre de nœuds malveillants.

La Fig. 1, en considérant 10% des nœuds comme malveillants, la valeur de coût de 0,50 a le meilleur résultat dans notre modèle. On observe lorsque le nombre de nœuds atteint à 60, un changement soudain s'est produit dans la valeur du TCR. Il n'y a pas beaucoup de différence dans la valeur de TCR sur la plage de 80 à 100 nœuds. Nous observons que TCR est toujours supérieur à 1, ce qui prouve la précision de nos filtres. Dans la Fig. 2, nous considérons que 20% des nœuds sont malveillants. La valeur de coût 0,25 dont les points sont représentés par des étoiles est plus significative. Lorsque le nombre de nœuds augmente jusqu'à 100, nous notons que les valeurs TCR sont diminuées. Dans les autres configurations, les valeurs de TCR sont considérées comme acceptables.

En résumé, nous avons observé des valeurs appropriées pour le TCR. Sur la base de ces résultats TCR, nous pouvons conclure que notre filtre offre une grande précision car les valeurs TCR sont toujours supérieures à 1, même avec un taux élevé de nœuds malveillants. Cela prouve que le modèle proposé est capable d'attribuer des scores précis à différents nœuds et garantit un taux élevé de détection de ces nœuds malveillants.

III. La Conclusion

Nous avons proposé un modèle de réputation décentralisé précis qui calcule les scores de comportement et évalue la fiabilité des nœuds dans les réseaux véhiculaires. Nous avons formulé le problème en utilisant un filtre bayésien. Ensuite, nous avons décrit notre stratégie de classification et calculé la précision du filtre proposé. Le modèle surveille le comportement des véhicules où chaque nœud peut décider d'interagir avec ses voisins en analysant leurs comportements. Nous avons effectué de nombreuses simulations pour illustrer la validité du modèle de réputation proposé. Les résultats ont montré un taux de détection intéressant concernant la précision et les valeurs de TCR dans diverses conditions de réseau.

Les auteurs remercient le MSER, le FEDER et la Région GRAND-EST pour le soutien financier de ce travail de recherche.

References

[1] M. A. Togou, A. Hafid, and L. Khoukhi, *A Novel CDS-Based Routing Protocol for Vehicular Ad Hoc Networks in Urban Environments*, 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, 2015, pp. 1-6, doi: 10.1109/GLOCOM.2015.7417266.

[2] Nabet, R. Khatoun, L. Khoukhi, J. Dromard and D. Gaïti, *Towards secure route discovery protocol in MANET*, Global Information Infrastructure Symposium - GIIS 2011, Da Nang, 2011, pp. 1-8, doi: 10.1109/GIIS.2011.6026717.

[3] H Khelifi, S. Luo, B. Nour, H. Moungla, Y. Faheem, R. Hussain, and A. Ksentini, *Named Data Networking in Vehicular Ad Hoc Networks: State-of-the-Art and Challenges*, IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 320-351, Firstquarter 2020, doi: 10.1109/COMST.2019.2894816.

[4] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga, and Y. Ji, *Decentralized Trust Evaluation in Vehicular Internet of Things*, IEEE Access, vol. 7, pp. 15980-15988, 2019.

[5] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, *MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles*, in IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3310-3322, April 2020, doi: 10.1109/JIOT.2020.2967568.