Confidentialité et sécurité renforcées dans les réseaux véhiculaires: solutions hybrides IA–Blockchain

Durée : 4 à 6 mois Début : Début 2026

1. Contexte et problématique

Les réseaux véhiculaires ad hoc (VANETs) représentent une composante essentielle des systèmes de transport intelligents (ITS), en permettant aux véhicules d'échanger en temps réel des informations critiques telles que la position, la vitesse, l'état du trafic ou encore des alertes de sécurité routière. Ces communications, qui reposent sur une architecture distribuée et hautement dynamique, visent à améliorer la fluidité de la circulation, à renforcer la sécurité routière et à favoriser l'émergence des véhicules autonomes.

Cependant, la nature ouverte et décentralisée des VANETs les rend particulièrement vulnérables à des menaces de sécurité. Parmi les principales attaques, on distingue l'usurpation d'identité (Sybil attack), l'injection de messages falsifiés, la falsification de coordonnées GPS, le déni de service (DoS/DDoS) ou encore l'écoute passive et l'analyse du trafic. Ces attaques compromettent non seulement la confidentialité et l'intégrité des données, mais elles peuvent également mettre en danger la sécurité physique des usagers de la route.

Ainsi, il devient impératif de concevoir des solutions robustes et intelligentes capables de détecter rapidement les comportements anormaux, de sécuriser les échanges d'informations et de prévenir les attaques futures. L'intégration de l'Intelligence Artificielle pour la détection proactive, combinée à la Blockchain pour garantir la traçabilité et l'immutabilité des données, ouvre de nouvelles perspectives de recherche et constitue l'axe principal de ce projet.

Mots-clés: VANETs –Sécurité des réseaux –Intelligence Artificielle –Blockchain– Détection d'attaques.

2. Objectifs du projet

- Étudier les techniques de sécurité dans les VANETs et les principaux types d'attaques.
- Utiliserl'IntelligenceArtificiellepourladétectionautomatiqued'attaques.
- Expérimenterl'utilisationdelaBlockchainpourgarantirl'intégritéetla traçabilité des données.
- Développer un modèle prédictif pour anticiper la probabilité d'attaques futures.

3. Méthodologie et Travaux attendus

- Étude bibliographique sur les réseaux VANETs, leurs vulnérabilités et les approches de sécurité basées sur l'IA et la Blockchain.
- Utilisation du dataset VeReMi Extension, contenant des scénarios simulés d'attaques dans les VANETs.
- Prise en main et prétraitement des données issues du dataset.
- Développement d'un modèle IA pour la détection des attaques.
- Intégrationd'unprototypeBlockchainafinderenforcerl'intégritéetla traçabilité des données.
- Expérimentation d'un modèle de régression pour la prédiction et l'anticipation des attaques.

4. Profil recherché

Étudiant·e en master ou en école d'ingénieur, motivé·e, disposant de solides bases en programmation Python (pandas, scikit-learn, TensorFlow/Keras), en apprentissage automatique et profond, ainsi que de connaissances de base en sécurité des réseaux.

Encadrement: Om Essaad Slama, Oum-El-Kheir Aktouf, Annabelle Mercier
Contact: om-essaad.slama@lcis.grenoble-inp.fr
Lieu : Laboratoire de Conception et d'Intégration des Systèmes de Valence (LCIS)

Références

K. Joseph, W. Michael, V. W. Rens, A. Kaiser, P. Urien, and K.Frank, "VeReMi extension: A dataset for comparable evaluation of misbehavior detection in VANETs." CC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020.

Slama, O. Tarhouni, M., Zidi, S. and Alaya, B., One Versus All Binary Tree Method to Classify Misbehaviors in Imbalanced VeReMi Dataset, In IEEE Access, , 11, pp.135944-135958. 10.1109/ACCESS.2023.3337378.

Bendiab, G., Hameurlaine, A., Germanos, G., Kolokotronis, N. and Shiaeles, S. (2023) 'Autonomous vehicles security: challenges and solutions using blockchain and artificial intelligence', IEEE Transactions on Intelligent TransportationSystems, Vol. 24, pp.3614–3637, doi: 10.1109/TITS.2023.32362.

W. Dhifallah, T. Moulahi, T. Mounira, S. Zidi, Intellig_block: Enhancing IoT security with blockchain-based adversarial machine learning protection, International Journal of Advanced Technology and Engineering Exploration, 10(106):106, September 2023, DOI: 10.19101/IJATEE.2023.10101465.