Republique Tunisienne
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Jendouba
Institut Supérieur d'Informatique du Kef

الجمهورية التونسية
وزارة التعليم العالي والبحث العلمي
جامعة جندوبة
المعهد العالي للإعلامية بالكاف

Proposition d'une nouvelle approche basée sur le machine learning pour la détection d'intrusions dans les réseaux véhiculaires intelligents (VANETs)

Encadrant académique: Dr. Anwer KALGHOUM

Email: anouar.kalghoum@isikef.u-jendouba.tn | anwer.kalghoum@gmail.com

Description:

Les réseaux véhiculaires intelligents (VANETs) jouent un rôle essentiel dans l'écosystème des systèmes de transport intelligents, en facilitant la communication entre véhicules et infrastructures. Cependant, en raison de leur nature dynamique et distribuée, les VANETs sont particulièrement vulnérables à divers types de cyberattaques, telles que les attaques de type Sybil, la falsification de messages et les attaques par déni de service. Ces menaces peuvent compromettre la sécurité des passagers et l'efficacité des systèmes de transport.

Les méthodes traditionnelles de détection d'intrusion peinent à répondre aux défis uniques des VANETs, tels que le besoin de détection en temps réel, la gestion de volumes massifs de données et l'adaptabilité à des scénarios d'attaque variés. Ce projet propose de développer une nouvelle approche utilisant des techniques de **machine learning** et d'**ensemble learning** pour améliorer la précision, la robustesse et la rapidité des systèmes de détection d'intrusion dans les VANETs.

L'ensemble learning, qui combine plusieurs modèles de machine learning pour améliorer les performances globales, sera au cœur de cette approche. Des techniques telles que le bagging (e.g., Random Forest), le boosting (e.g., Gradient Boosting Machines, XGBoost), et les ensembles empilés (stacked ensembles) seront explorées pour concevoir un système de détection performant et résilient.

Objectifs:

1. **Étude de l'état de l'art des solutions existantes:**
   - Analyse des vulnérabilités et des attaques courantes dans les VANETs.
   - Examen des méthodes de détection d'intrusions actuellement utilisées, incluant les approches basées sur les signatures, l'analyse comportementale, les méthodes statistiques, l'apprentissage automatique, et l'ensemble learning.

2. **Proposer une nouvelle approche basée sur le machine learning et l'ensemble learning:**

- Concevoir un modèle de détection d'intrusion qui combine des techniques d'apprentissage supervisé et non supervisé pour améliorer la précision et réduire les faux positifs.
- Utiliser des techniques d'ensemble learning, comme le bagging et le boosting, pour renforcer les performances du système.

3. **Développer un modèle de détection efficace et adaptatif :**
   - Intégrer le modèle dans un environnement VANET simulé ou réel.
   - Tester et évaluer la capacité du modèle à détecter des attaques en temps réel tout en minimisant les coûts computationnels.

4. **Évaluer et comparer les performances du modèle proposé :**
   - Comparer les résultats obtenus avec ceux des méthodes existantes en termes de précision, taux de faux positifs et temps de détection.
   - Évaluer l'adaptabilité du système à différents types d'attaques et sa robustesse face aux variations des données.

Résultats attendus:

- Un modèle de détection d'intrusion basé sur l'ensemble learning, optimisé pour les environnements VANETs.
- Une réduction significative des taux de faux positifs par rapport aux méthodes existantes.
- Un système capable de détecter des intrusions complexes en temps réel avec une grande précision.

Références:

1. **Rahman, M. S., et al. (2024).** "Advanced Ensemble Learning Techniques for Intrusion Detection in Vehicular Ad Hoc Networks." *IEEE Transactions on Intelligent Transportation Systems.* DOI
2. **Islam, S. R., et al. (2024).** "Optimizing Security in VANETs Using Federated and Ensemble Learning." *Elsevier Vehicular Communications.* DOI
3. **Ahmed, M. U., et al. (2024).** "Intrusion Detection for VANETs: Exploring the Synergy of Machine Learning and Ensemble Approaches." *Springer Lecture Notes in Computer Science.* DOI
4. **Boualouache, A., et al. (2024).** "A Review on Security and Machine Learning Techniques for Vehicular Networks." *International Journal of Communication Systems.* DOI
5. **Hodo, E., et al. (2024).** "Real-Time Detection of VANET Attacks Using Boosting Algorithms." *arXiv preprint arXiv:2401.08564.* arXiv

Mot-clés: Machine learning, ensemble learning, détection d'intrusion, VANETs, sécurité des réseaux, transport intelligent, bagging, boosting, réseaux véhiculaires