# Smart models for security enhancement in the internet of vehicles

Houda Amari

Normandie Université

UNIVERSITÉ CAEN NORMANDIE

# THÈSE

**Pour obtenir le diplôme de doctorat**

Spécialité **INFORMATIQUE**

Préparée au sein de l'**Université de Caen Normandie**

En cotutelle internationale avec l'**l'Université de Sfax, TUNISIE**

## SMART MODELS FOR SECURITY ENHANCEMENT IN THE INTERNET OF VEHICLES

Présentée et soutenue par

**HOUDA AMARI**

**Thèse soutenue le 19/12/2023**

devant le jury composé de :

| | | |
|---|---|---|
| MME LEILA BEN AYED | Professeur - Université de la Manouba Tunis - Tunisie | Rapporteur du jury |
| M. PASCAL LORENZ | Professeur des universités - Université de Haute-Alsace | Rapporteur du jury |
| M. ZAKARIA ABOU EL HOUDA | Chercheur - Université du Québec - INRS | Membre du jury |
| MME SARA BERRI | Maître de conférences - CY Cergy Paris Université | Membre du jury |
| MME NADIA BOUASSIDA | Professeur - l'Université de Sfax | Membre du jury |
| M. PHILIPPE DESCAMPS | Professeur des universités - ENSICAEN | Président du jury |
| M. LYES KHOUKHI | Professeur des universités - ENSICAEN | Directeur de thèse |
| MME LAMIA HADRICH BELGLITH | Professeur - l'Université de Sfax | Co-directeur de thèse |

Thèse dirigée par **LYES KHOUKHI** (GREYC ALGORITHMIQUE) et **LAMIA HADRICH BELGLITH** (l'Université de Sfax)

MIRIAM

GREYC
Laboratoire de recherche en sciences du numérique

# *Abstract*

With the major progress in Intelligent Transportation Systems (ITS), there has been an exponential interest in technological advancements of Internet of Vehicles (IoV), attracting the attention of numerous researchers from academia and industry. IoV technology aims to enhance transport efficiency, passenger safety, and comfort by exchanging traffic and infotainment information to connected vehicles. The multitude of network access technologies, the exceptionally high mobility of connected vehicles and their high density in urban areas, and the predominance of wireless communications make the IoV ecosystem a complex, vulnerable and heterogeneous network with very dynamic characteristics, some of which are difficult to predict and subject to scalability and threats problems. Many entities compose its architecture (connected vehicles, humans, roadside units (RSUs), ITS). Moreover, it presents different communication types to confirm its connectivity and vulnerability. However, this diversity leads to new security requirements that seem challenging to consider and enlarge the attack surface of such networks. Therefore, disseminating malicious messages/entities within the network significantly reduces the network performance and becomes a threat to passengers and vulnerable pedestrians. Accordingly, security mechanisms should be considered to secure communications in vehicular networks. This thesis aims to develop novel models to enhance the security aspects of the IoV ecosystem dealing with diverse attacks, including DDoS attacks, while preserving users' privacy.



***Key words :*** Internet of Vehicles, Software-defined network, Security attacks detection, Trust management, Reputation system, Blockchain.

# *Résumé*

Avec les progrès réalisés au cours de la dernière décennie dans les Systèmes de Transport Intelligents (STI), les progrès technologiques dans le domaine véhciculaire à connu une évolution qui a donné naissance au paradigme prometteur de l'Internet des véhicules (IoV), attirant l'attention de nombreux chercheurs et inudstriels. Il est à noter que l'Internet des véhicules (IoV) vise à améliorer l'efficacité des transports, la sécurité et le confort des passagers en échangeant des informations sur la circulation et l'infodivertissement avec des véhicules connectés. La multitude de technologies d'accès aux réseaux, la mobilité exceptionnellement élevée des véhicules connectés et leur forte densité en zone urbaine, ainsi que la prédominance des communications sans fil font de l'écosystème IoV un réseau complexe, vulnérable et hétérogène aux caractéristiques très dynamiques de l'environnement véhiculaire. De nombreuses entités composent son architecture (véhicules connectés, humains, unités routières. De plus, les réseaux véhiculaires présentent différents types de communication pour confirmer sa connectivité et sa continuité. En conséquence, de nombreux messages critiques pour la sécurité à faible latence sont générés et échangés au sein du réseau. Cependant, cette diversité conduit à de nouvelles exigences de sécurité qui semblent difficiles à prendre en compte et à élargir la surface d'attaque de tels réseaux. Par conséquent, la diffusion de messages/entités malveillants au sein de l'IoV réduit considérablement les performances du réseau et devient une menace pour les passagers et les piétons vulnérables. En conséquence, des mécanismes de sécurité devraient être envisagés pour sécuriser les communications dans l'IoV. Cette thèse vise à proposer de nouveaux modèles pour améliorer les aspects de sécurité de l'écosystème IoV face à diverses attaques, y compris les attaques DDoS, tout en préservant la confidentialité des utilisateurs.



***Mots clés :*** Internet des véhicules, Software Defined Network, detection des attaques, gestion de la confiance, système de réputation, Blockchain.

# Acknowledgments

I would like to take this opportunity to express my deepest gratitude to all the people who made it possible for me to achieve my thesis. First and foremost, I am deeply thankful to my supervisor Prof. Lyes Khoukhi, who encouraged and supported me throughout my Ph.D. degree and was always an admirable motivation to swing for the fences. I can not thank you enough for having confidence in me, it wouldn't have been possible to accomplish this goal without your efforts. I would also like to say thank you to my supervisor Prof. Lamia Hadrich Belguith, for her guidance throughout the degree.

Throughout my Ph.D. degree, my colleagues and the admin staff have been extremely considerate and cooperative. I want to acknowledge them for their continuous support and always cheering me up.

To my friends Nessrine, Safa and Wahiba, your words of encouragement during moments of doubt and your shared laughter during breaks provided the balance I needed to navigate the challenges of this research.

To my friend Kamel, i am grateful for the late-night study sessions, the brainstorming sessions, and the shared excitement when breakthroughs were made. Your camaraderie has made this academic endeavor a memorable and enriching experience.

Finally, yet most importantly, I express my profound appreciation to my family for their unwavering love and support for me in my most incredible accomplishment.

To my loving parents and my siblings, words cannot express how grateful I am for all your love, support, and encouragement along the way. I couldn't possibly have done this without you.

# Dedication

A SPECIAL THANK YOU goes to MY FATHER MOHAMMED AMARI,
To my strategic partner in every step of this endeavor, my constant companion and my best friend, My motivation has been the desire to make you more proud of me ! Your belief in my abilities, your enduring encouragement, and your unwavering support throughout my academic journey have been a constant source of strength. Dad, your resilience and work ethic have been a constant source of inspiration. Your wisdom and guidance have shaped not only my academic pursuits but also the person I am becoming. Thank you, for being my role model, my mentor, and my biggest supporter. This achievement is as much yours as it is mine.

TO MY DEAREST MOTHER, HABIBA AMARI,
As I reflect on the pages of this thesis, I see not only my academic achievements but also the reflection of your boundless love and your sacrifices that have been the bedrock upon which my educational journey has been built. I am profoundly grateful for the countless sacrifices you have made to ensure my education and success. Your sacrifices have not gone unnoticed, and this work is a tribute to your enduring love and dedication to my well-being.

To my beloved sister, MOUNA, and my two brothers, KHALED and HOUSSEM,
As we celebrate the completion of this chapter, I dedicate this achievement to each of you. Your love and support have been instrumental in my success, and I am profoundly grateful for the bond we share. Together, as siblings, you formed an unbreakable support system. Your sacrifices, understanding, and shared pride in my accomplishments have made this achievement not only mine but ours.

I dedicate this thesis to the honorable Professor ANIS JARBOUI,
In moments of doubt, you provided reassurance ; in times of celebration, you shared in the joy. Thank you for being one of my biggest supporters since day one. Your contribution to my journey is immeasurable, and I am profoundly grateful for the impact you've had on my life and this thesis.

THANK YOU ALL for being a part of this special journey !

With deepest gratitude and love,

Houda

# Contents

**List of Figures** 10

**List of Tables** 11

**List of Publications** 12

**List of Abbreviations** 13

**INTRODUCTION** 15

**1 OVERVIEW ON IoV** 19
- 1.1 Introduction . . . 20
- 1.2 Definition of IoV . . . 20
  - 1.2.1 Architecture's Components . . . 22
- 1.3 Software-Defined Networking Based IoV . . . 24
  - 1.3.1 Software-Defined Networking (SDN) . . . 24
  - 1.3.2 Software-Defined Vehicular Network (SDVN) . . . 25
- 1.4 Security and privacy for IoV . . . 26
  - 1.4.1 Security requirements in IoV . . . 27
  - 1.4.2 Privacy requirements in IoV . . . 27
  - 1.4.3 Balance between Security and Privacy . . . 28
- 1.5 Conclusion . . . 28

**2 VEHICULAR NETWORKS' TRUST MANAGEMENT** 29
- 2.1 Introduction . . . 30
  - 2.1.1 Contributions of this work . . . 30
  - 2.1.2 Structure of the chapter . . . 30
  - 2.1.3 Research Methodology . . . 34
- 2.2 Overview of Trust Management Mechanisms . . . 35
  - 2.2.1 Characteristics . . . 35
  - 2.2.2 Metrics . . . 36
  - 2.2.3 Computation modules . . . 36
- 2.3 Existing Surveys . . . 37
  - 2.3.1 Contributions of existing surveys . . . 37
  - 2.3.2 Comparison with our work . . . 37
- 2.4 Issues . . . 38
  - 2.4.1 Security Issues . . . 38
  - 2.4.2 Trust management Issues . . . 38
  - 2.4.3 Security attacks in IoV. . . . 39
- 2.5 Classification . . . 41
  - 2.5.1 Entity-based schemes . . . 41
  - 2.5.2 Hybrid schemes . . . 43
  - 2.5.3 Technology-based classification . . . 44
- 2.6 Discussion . . . 49
  - 2.6.1 Summary . . . 49
  - 2.6.2 Comparison . . . 49
- 2.7 Future Work . . . 54
  - 2.7.1 Federated Learning-based solutions . . . 54
  - 2.7.2 Clustering approaches . . . 54
  - 2.7.3 Energy consumption . . . 54

2.7.4 Emerging technologies . . . 55
2.8 Conclusion . . . 55

**3 PREDICTION AND DETECTION OF DDOS ATTACKS IN SDVN 57**
3.1 Introduction . . . 58
3.2 A Robust SDVN Framework for Mitigating DDoS Attacks . . . 58
3.2.1 Brief Overview . . . 58
3.2.2 Proposed work . . . 59
3.3 Proposed model's performance . . . 60
3.4 Evaluation . . . 63
3.5 Discussions . . . 66
3.6 Conclusion . . . 67

**4 TRUST MANAGEMENT FOR CONNECTED VEHICLES WITH PRIVACY PRESERVING 69**
4.1 Introduction . . . 70
4.2 System model . . . 70
4.2.1 Proposed Blockchain . . . 72
4.2.2 Network Components . . . 73
4.3 Adversary model . . . 73
4.3.1 Adversary RSU . . . 73
4.3.2 Adversary vehicles . . . 75
4.4 Vehicles' Pseudonyms Management . . . 75
4.4.1 System initialization (SDNC, RSUC, Vehicles) . . . 75
4.4.2 Vehicles' and RSUCs' registration . . . 75
4.4.3 Vehicle authentication . . . 76
4.4.4 Message authentication . . . 77
4.5 Trust Model . . . 78
4.5.1 Trust system's process . . . 78
4.5.2 Trust Process . . . 79
4.6 Implementation . . . 80
4.7 Security analysis . . . 81
4.8 Conclusion . . . 82

**5 Federated Learning-based Intrusion Detection System for Connected Vehicles 85**
5.1 Introduction . . . 86
5.2 Related Work and Background . . . 86
5.2.1 Blockchain-based IDS . . . 87
5.2.2 Machine and Deep Learning IDS . . . 87
5.3 System Overview . . . 88
5.4 System Model . . . 88
5.4.1 Network components . . . 88
5.4.2 Powers of Smart Contracts . . . 91
5.4.3 Adversary Model . . . 92
5.5 Proposed VFed-IDS Architecture . . . 92
5.5.1 Classification Step . . . 92
5.5.2 Malicious vehicles detection . . . 93
5.6 Simulations . . . 93
5.6.1 Experimental setup . . . 93
5.6.2 Description of NSL-KDD dataset . . . 95
5.6.3 Attacks types . . . 97
5.7 Results' Discussion . . . 99
5.7.1 Impact of rounds number on model's metrics . . . 99
5.7.2 ROC Curve . . . 112
5.8 Open issue . . . 116
5.8.1 Federated Learning Clients' Selection . . . 116
5.8.2 Rounds' total number of FL process . . . 117
5.9 Conclusion . . . 117

**6 CONCLUSION AND PERSPECTIVES 119**

**ANNEX** **123**

**REFERENCES** **131**

# Table des figures


1.1 Basic Vehicular Network Architecture. . . . 21
1.2 Vehicle-to-everything (V2X) communications types in IoV. . . . 23
1.3 SDN architecture. . . . 25
1.4 Proposed hierarchical SDN-based Vehicular Network (SDVN) architecture. . . . 26

2.1 Our Survey organization. . . . 34
2.2 Trust management main pillars. . . . 35

3.1 Security model for hierarchical SDVN architecture. . . . 59
3.2 OpenFlow Switch under DDoS attack. . . . 61
3.3 Behavior ranges thresholds . . . . 61
3.4 Behavior ranges thresholds . . . . 63
3.5 The distribution of vehicles at time t. . . . 64
3.6 The distribution of vehicles at time t. . . . 65
3.7 The distribution of vehicles at time t+1. . . . 65
3.8 The distribution of vehicles at time t+2. . . . 66
3.9 The distribution of vehicles at time t+3. . . . 66
3.10 The distribution of vehicles at time t+4. . . . 66

4.1 Vehicles' ratings generation based on Bayesian Inference Filter. . . . 73
4.2 System Architecture. . . . 74
4.3 System's initialization, vehicle, and RSUC registration, and exchanged messages diagram. 76

5.1 Federated Learning and Blockchain based IDS for Connected Vehicles . . . . 90
5.2 Our smart contract VFed-SC process. . . . 91
5.3 NSL-KDD dataset distribution. . . . 98
5.8 Accuracy rate of 25 vehicles. . . . 99
5.4 Accuracy rate evolution of SDNC with MLP model while varying number of vehicles. . . . 100
5.5 Accuracy rate evolution of 10 vehicles with varying number of rounds. . . . 101
5.6 Accuracy rate evolution of SDNC with varying number of vehicles. . . . 102
5.7 Accuracy rate of 10 vehicles. . . . 102
5.9 Loss rate of 10 vehicles. . . . 103
5.10 Loss rate of 25 vehicles. . . . 103
5.11 Precision score evolution of vehicles per rounds with MLP model. . . . 104
5.12 Precision scores of 10 vehicles with MLP and RNN models. . . . 105
5.13 Precision scores of 25 vehicles with MLP and RNN models. . . . 105
5.14 Recall scores of 10 vehicles with MLP and RNN models. . . . 106
5.15 Recall scores of 25 vehicles with MLP and RNN models. . . . 106
5.16 Recall Score evolution of vehicles per rounds. . . . 107
5.17 F1 scores of 10 vehicles. . . . 108
5.18 F1 scores of 25 vehicles. . . . 108
5.19 F1 score evolution of vehicles per rounds with MLP model. . . . 109
5.20 SDNC Confusion Matrix evolution with 10 vehicles with MLP model. . . . 110
5.21 SDNC Confusion Matrix evolution with 25 vehicles with MLP model. . . . 110
5.22 SDNC Confusion Matrix evolution with 50 vehicles with MLP model. . . . 110
5.23 SDNC Confusion Matrix evolution with 100 vehicles with MLP model. . . . 111
5.24 SDNC Confusion Matrixes' Evolution with MLP model while varying vehicles' number. . 111
5.25 SDNC Confusion Matrixes' Evolution with MLP model while varying rounds' number. . . 112
5.26 Loss rate evolution of 10 vehicles varying rounds number with MLP model. . . . 113
5.27 Accuracy Score of VFed-IDS and other ML/DL models. . . . 114

5.28 The VFed and ML accuracy results of MLP and RNN models. . . . . 114
5.30 ROC Curve Evolution of SDNC with 10 vehicles in 25 rounds with MLP model. . . . . 115
5.29 The ROC Curve concept. . . . . 115
5.31 ROC Curve Evolution of SDNC with 25 vehicles in 25 rounds with MLP model. . . . . 116
5.32 ROC Curve Evolution of SDNC with 50 vehicles in 25 rounds with MLP model. . . . . 116
5.33 ROC Curve Evolution of SDNC with 100 vehicles in 25 rounds with MLP model. . . . . 116

# Liste des tableaux


2.1 **Security services in IoV.** . . . 31
2.2 **Privacy requirements in the IoV.** . . . 32
2.3 **Existing surveys on Vehicular networks.** . . . 33
2.4 **Comparison of our work with different trust surveys.** . . . 38
2.5 **Threats and attacks regarding security in Vehicular networks.** . . . 42
2.6 **Basic trust managements schemes in Vehicular networks.** . . . 45
2.7 **Emerging technology-based trust management schemes in Vehicular networks.** 50
2.8 **AI-based trust management schemes in Vehicular networks.** . . . 51
2.9 **Comparison of different surveyed trust management schemes in Vehicular networks.** . . . 52
2.10 **Continued Table.9** . . . 53

3.1 Repartition of nodes in the network. . . . 64

4.1 Cost and Security analysis of our smart contract-based framework . . . 81

5.1 Related works. . . . 88
5.2 Used symbols . . . 89
5.3 List of Features in NSL-KDD Dataset . . . 94
5.5 Existing samples in NSL-KDD dataset. . . . 95
5.4 Scenarios details. . . . 95
5.6 NSL-KDD Train and NSL-KDD Test dataset details. . . . 96
5.7 Attack Categories, Sub-Classes, and Descriptions in NSL-KDD Dataset . . . 96
5.8 Confusion Matrix . . . 96
5.9 Environment setup . . . 98

# List of Publications

## International Conferences

- **Houda Amari**, Zakaria Abou El Houda, Lyes Khoukhi and Lamia Hadrich Belguith." VFed-IDS : Federated Learning and Blockchain for Cyber-threats Detection in Connected Vehicles" In : IEEE International Conference on Communications **(IEEE ICC'24, Class B)**, 2023. **(Submitted)**

- **Houda Amari**, Lyes Khoukhi and Lamia Hadrich Belguith."Prediction and detection model for hierarchical Software-Defined Vehicular Network" In : IEEE 47th Conference on Local Computer Networks, **(IEEE LCN'22, Class B)**,2022.

- **Houda Amari**, Wassef Louati, Lyes Khoukhi and Lamia Hadrich Belguith. "Securing Software-Defined Vehicular Network Architecture against DDoS attack" In : IEEE 46th Conference on Local Computer Networks,**(IEEE LCN'21, Class B)** 2021.

- **Houda Amari**, Wassef Louati, Lyes Khoukhi and Lamia Hadrich Belguith."TCP Incast Solutions in Data Center Networks : Survey" In : the International conference on Local Computer Networks (HIS),**(HIS'20, Class C)** 2020.

## Journal papers

- **Houda Amari**, Zakaria Abou El Houda, Lyes Khoukhi and Lamia Hadrich Belguith." VFed-IDS : Federated Learning and Blockchain for Cyber-threats Detection in Connected Vehicles" In : The International Journal of Computer and Telecommunications Networking, 2023. **(Under submission)**

- **Houda Amari**, Zakaria Abou El Houda, Lyes Khoukhi and Lamia Hadrich Belguith."Trust Management in Vehicular Ad-Hoc Networks : Extensive Survey" In : the International conference on Local Computer Networks **(IEEE ACCESS, Scimago Quartile Q1)**, 2023. **(Published)**

- **Houda Amari**, Zakaria Abou El Houda, Lyes Khoukhi and Lamia Hadrich Belguith."A Decentralized Blockchain-based Trust Management System for Connected Vehicles" In : The International Journal Of Management And Network, 2023. **(Under Reviewing)**

# List of Abbreviations

| Abbreviation | Meaning |
|---|---|
| **ITS** | the Intelligent Transport Systems |
| **IoV** | Internet of Vehicle |
| **MANET** | Mobile Ad-hoc Network |
| **OBU** | On Board Unit |
| **RSU** | Road-Side Unit |
| **AU** | Application Unit |
| **SDN** | Software-Defined Network |
| **ML** | Machine Learning |
| **DL** | Deep Learning |
| **BS** | Basic Station |
| **V2V** | Vehicle to Vehicle communication |
| **V2I** | Vehicle to Infrastructure |
| **V2X** | Vehicle to everything |
| **C-V2X** | Cellular Vehicle-to-everything |
| **3GPP** | Third Generation Partnership Project |
| **SDNC** | Software-Defined Networks Controller |
| **OF** | OpenFlow |
| **QoS** | Quality of Service |
| **API** | Application programming interface |
| **TA** | Trusted Authority |
| **PKI** | Public Key Infrastructure |
| **DoS** | Denial of Service |
| **DDoS** | Distributed Denial of Service |
| **GPS** | Global Positioning System |
| **CH** | Cluster Head |
| **CM** | Cluster Member |
| **SDVN** | Software-Defined Vehicular Network |
| **DSRC** | Dedicated Short Range Communication |
| **RSUC** | Road Side Units Controller |
| **BSC** | Basic Stations Controller |
| **WAVE** | Wireless Access in Vehicular Environments |
| **MSC** | Management Smart Contract |
| **TSC** | Trust Smart Contract |
| **RSC** | Revoke Smart Contract |
| **TOD** | Transaction-ordering dependence |
| **FL** | Federated Learning |

# INTRODUCTION

## Context

In spite of considerable progress in technology and policy development aimed at improving road safety, transportation systems worldwide continue to grapple with significant safety and efficiency challenges. The annual global road traffic fatality toll, as reported by the organization of world's health (WHO) [1], is a staggering 1.35 million, translating to nearly 3,700 lives lost daily in accidents encompassing diverse modes of transport. Road traffic damage is the leading cause of death across all age bunches and represents the primary cause of mortality for individuals aged 5 to 29 years.

To address these pressing issues, Intelligent Transportation Systems (ITS) propose equipping vehicles and transport infrastructure with secure, robust, and reliable communication capabilities. The overarching goal of ITS is to provide safer road environments by reducing accidents, optimizing travel times, minimizing pollution, enhancing passenger comfort through multimedia and infotainment services, and bolstering security against cyber threats. Combining communication capabilities with sensor-based detection and perception integrated into vehicles enables the development of diverse ITS services and a multitude of use cases. Notable among these services is Cooperative Collision Avoidance (CCA), which allows vehicles to exchange critical mobility information to prevent accidents. Another pivotal service is Cooperative Perception, offering a comprehensive view of the surroundings by aggregating data from neighboring vehicles, aiding in effective decision-making and trajectory planning. ITS also introduces Platooning, the cooperative grouping of vehicles to save fuel, enhance safety, and optimize road usage.

Urban areas grapple with traffic-related challenges, and vehicular networks stand as pivotal solutions. The conjunction of Big Data with cloud and edge computing and the Internet of Things (IoT) is improving the evolution of these networks [2]. The Internet of Vehicles (IoV) has garnered substantial attention from both academia and industry, shaping the trajectory of the next generation of vehicles. These vehicles will inherently possess connectivity, enabling communication with various Intelligent Transport System components, including other vehicles, pedestrians, and infrastructure elements (such as On-Board Units, Roadside Units, Base Stations, and the Cloud). The result is a cohesive vehicular network that plays a vital role in sustaining the IoV ecosystem, aiming to deliver the requisite network connectivity performance.

The IoV can enhance traffic safety and efficiency by the Vehicle to Everything communications. V2X communication involves a spectrum of interactions wherein connected vehicles utilize wireless communication to exchange information with other vehicles, the surrounding infrastructure, onboard sensors, personal devices, and cloud servers. The applications of V2X span safety-critical functionalities, including congestion management, crash prevention, and collision notifications, as well as non-safety applications such as navigation, anti-theft measures, and entertainment services. These applications, in conjunction with vehicle-embedded sensors, bolster traffic management and road safety by disseminating collision warnings, emergency brake notifications, hazard alerts, obstacle warnings, and traffic congestion information. Given the sensitivity of these applications, ensuring the security and reliability of exchanged information is paramount, as malicious actors can potentially disrupt the communication, leading to accidents and loss of lives.

Tesla has been notable for its cybersecurity measures, particularly its complex challenge system designed to thwart conventional methods of attacking remote unlock systems. Nevertheless, a recent discovery has revealed a sophisticated relay attack, which could enable a physical attacker to unlock and steal a Tesla Model Y within seconds.

The expanding prominence of IoV in recent years is further underscored by the rapid proliferation of wireless devices on roadways. Estimates suggest that by 2025, over 500 million connected vehicles will be in operation [**?**]. The sheer scale and dynamism of these networks pose challenges in meeting the stringent requirements of low latency, high mobility, top-tier security, and massive connectivity, all integral to the 5G/6G network. The inherently mobile and decentralized architecture of IoV makes it susceptible to security vulnerabilities, both from insiders and outsiders. To address these challenges, researchers from academia and industry have proposed security solutions grounded in cryptography. However, these solutions have primarily demonstrated their efficacy against outsider attacks, leaving insider attacks as a considerable concern.

In 2017, a group of Chinese security researchers [4] successfully hacked a Tesla Model X, gaining remote control over the car's brakes and the ability to open and close doors and trunk while synchronizing the lights to music from the car's radio, a display they humorously labeled "the unauthorized Xmas show." In a more recent development in 2022, a security consultant, Josep Pi Rodriguez, uncovered a complex relay attack on a Tesla Model Y [5]. This attack required two perpetrators, with one in proximity to the vehicle and the other close to the car owner, who possessed an NFC keycard or a mobile phone with a Tesla virtual key. These Near-Field Communication (NFC) keycards are used by Tesla owners for unlocking their vehicles and starting the engine. However, the car's manual advises keeping the NFC keycard as a backup. The attack involved the deployment of malicious software via the car's web browser through a series of intricate exploits, resulting in remote control of the vehicle via both Wi-Fi and cellular connections.

The automotive industry at large has faced similar challenges, with Nissan having to withdraw its application for the Leaf electric car due to security vulnerabilities. Also, about 1.4 million vehicles were placed by Fiat Chrysler Automobiles due to hackers' ability to attain electronic access to the cars and control brakes and acceleration via a software's security weakness.

As noted earlier, the IoV is particularly susceptible to attacks due to its high mobility and dynamic nature. This vulnerability poses a significant risk, potentially allowing for the manipulation of safety-critical messages and communication delays. These issues could ultimately contribute to road accidents and, tragically, the loss of human lives. The growing openness and unrestricted access within vehicular networks heighten their susceptibility to attacks. Hence, the imperative to enhance the security of the advanced IoV framework, addressing various attack types, whether insider or outsider, active or passive, becomes paramount. Furthermore, concerns regarding the misuse of private data by network users necessitate the exploration of innovative security solutions, constituting a significant domain of research.

## Motivations

Creating resilient vehicular security models is crucial to prevent the dissemination of tampered safety-critical messages. Such models can thwart malicious vehicles from broadcasting falsified data by implementing intelligent security measures rooted in stochastic models and emerging technologies like Blockchain, Software-Defined Networks (SDN), and the formidable capabilities of Machine Learning (ML). These models must adapt to the dynamic nature of the Internet of Vehicles (IoV), identifying anomalies, safeguarding privacy, and proactively guarding against a wide spectrum of threats. The primary goal is to bolster the security and safety of connected vehicles and their occupants. This involves establishing a reliable system where occupants can confidently trust the identity of the sender and the information being exchanged. It is imperative to identify and neutralize any malicious vehicles before they can pose a threat to the network. Imagine the catastrophic consequences if a malicious vehicle were to tamper with a collision avoidance warning, leading to fatal accidents and loss of human lives.

Traditional security mechanisms often fall short in addressing the unique characteristics of IoV comprehensively, especially in specific IoV scenarios. While cryptographic schemes are frequently employed to mitigate adversarial behavior from rogue vehicles, additional measures are necessary to evaluate the credibility of authenticated vehicles. Traditional security requirements like confidentiality, integrity, authentication, and availability remain critical.

Furthermore, specific actions can be tailored to the requirements of IoV in a given scenario, such as auditing for information tracking and trustworthiness. Incorporating stochastic models like Markov chains can capture the dynamic nature of vehicular networks and enable informed decisions based on current states and transition probabilities. These models can forecast the future security states of connected vehicles by analyzing past transitions and events, offering proactive security measures.

Integrating Software-Defined Networking (SDN) with vehicular networks unifies their control planes, allowing IoV to leverage diverse access technologies while managing network resources efficiently. This flexibility is vital for providing communication services that adhere to security requirements within IoV.

The concept of trust has gained prominence in addressing insider attacks within vehicular networks. Trust-based vehicular security models prevent the exchange of malicious messages and facilitate their revocation. Trust management evaluates data and entities by assigning trust values to ensure road safety. Blockchain integration in the trust management process establishes a decentralized platform with an up-to-date trust value ledger accessible to participating nodes. Vehicles and Roadside Units (RSUs) can request the trust value of any other node.

Developing an Intrusion Detection System (IDS) grounded in Federated Learning and Blockchain for vehicular networks offers a comprehensive approach to security and privacy. This approach combines decentralized learning, privacy preservation, tamper-resistant ledger technology, and collaborative defense mechanisms to create a secure and adaptable IDS system that can effectively safeguard vehicular networks against a variety of security threats while upholding the privacy of network participants. Such an approach is paramount for ensuring the safety, security, and trustworthiness of vehicular communication systems.

In light of these considerations, our research endeavors to explore the development of intelligent models to secure communications between connected vehicles and address network scalability. Our security models not only provide conditional privacy for drivers but also enhance the autonomous behavior of connected vehicles.

## Organisation

In this thesis, we delve into the field of the Internet of Vehicles in an effort to fully comprehend the capability of vehicular networks to tackle the security obstacles presented by traditional connected vehicles. We introduce an overview of IoV. We talk generally about its network's components, communications types, characteristics and domain of applications. We also overview the security and privacy-preserving in such networks. The, we talk about the importance of integrating the Software-Defined Network paradigm in IoV. We outline the powers of combining this technology in IoV. We present our proposed hierarchical SDN-based Vehicular Network architecture (SDVN). We outline the benefits of having hierarchical architecture.

In this phase of our study, we conduct a comprehensive review of the literature on trust management within the Internet of Vehicles (IoV) context. We examine applicable schemes and explore existing surveys on the security of connected vehicles, providing a general overview of trust concepts. Additionally, we analyze security and trust challenges specific to vehicular networks and classify relevant trust management approaches based on technology and classical criteria. A qualitative comparison is performed to evaluate these approaches. Finally, we outline potential future research directions and perspectives in IoV trust management. This extensive review is the foundation for our subsequent research efforts to enhance security and trust within the IoV ecosystem.

Our initial contribution involves the implementation of a hierarchical architecture designed to enhance the security of Software-Defined Vehicular Networks (SDVN). In conjunction with this architecture, we introduce a secure framework for anticipating and identifying Distributed Denial of Service (DDoS) attacks. This model utilizes a Markov stochastic chain to analyze the network node's behavior. Through comprehensive simulations, we deliver compelling evidence that our model excels in mitigating DDoS attacks, reaching a significant level of reliability in defending vehicular networks.

Our second major contribution lies in the introduction of a fully decentralized trust management framework based on Blockchain technology. This innovative framework relies on multiple smart contracts to establish trust and enhance security within future Software-Defined Vehicular Networks (SDVN). The framework functions in a completely distributed, transparent, secure, tamper-proof, and trustworthy manner. We have meticulously implemented, tested, and deployed this system on the Ethereum network. The experimental results obtained underscore the system's remarkable attributes, including adaptability, flexibility, security, efficiency, and cost-effectiveness. Consequently, this framework emerges as a highly promising solution for the development of novel decentralized trust management systems within the realm of Intelligent Transportation Systems (ITS).

Our third principal contribution centers on the proposal of VFed-IDS, a decentralized, secure, flexible, scalable, and robust architecture based on Blockchain and Federated Learning. This innovative architecture is specifically designed to bolster privacy preservation in connected vehicles. VFed-IDS operates through three primary layers : the central layer, the local layer, and the Blockchain layer. The central layer features the SDN Controller, responsible for training and aggregating the global model, while the local layer consists of vehicles training their respective local models using private local datasets. The Blockchain layer assumes the critical role of managing transaction encryption between the central and local layers. Moreover, it introduces a smart contract, VFed-SC, tasked with overseeing the list of authenticated and collaborating vehicles within the Federated Learning (FL) process. This comprehensive architecture

represents a significant advancement in the realm of privacy protection for connected vehicles, promising increased security and efficiency within this dynamic environment.

We end this thesis by presenting a conclusion and some perspectives.

CHAPITRE 1

# OVERVIEW ON IoV

## Table des matières


1.1 Introduction . . . . . 20
1.2 Definition of IoV . . . . . 20
1.2.1 Architecture's Components . . . . . 22
1.3 Software-Defined Networking Based IoV . . . . . 24
1.3.1 Software-Defined Networking (SDN) . . . . . 24
1.3.2 Software-Defined Vehicular Network (SDVN) . . . . . 25
1.4 Security and privacy for IoV . . . . . 26
1.4.1 Security requirements in IoV . . . . . 27
1.4.2 Privacy requirements in IoV . . . . . 27
1.4.3 Balance between Security and Privacy . . . . . 28
1.5 Conclusion . . . . . 28

## 1.1 Introduction

In the contemporary era characterized by rapid developments, Intelligent Transportation Systems (ITS) have attained unprecedented levels of sophistication. A particularly notable aspect of this progress is the rise of the Internet of Vehicles (IoV), a domain that has seen significant growth thanks to the rapid advancements in wireless communication technologies. IoV represents an emerging application of ad-hoc networks, where interconnected vehicles serve as mobile nodes within a dynamic network. What sets IoV apart and makes it increasingly popular are its unique characteristics. IoV facilitates real-time communication between moving vehicles, enabling the exchange of critical information related to traffic conditions, road status, weather updates, accident reports, and other pertinent data. This communication benefits not only the vehicles themselves but also their drivers, enhancing the overall driving experience. One of IoV's primary objectives is to mitigate the risk of accidents and other disruptions on the road. By sharing and disseminating essential information, it contributes to safer and more efficient traffic management. Nevertheless, various aspects of IoV still require extensive research and development. Key areas of focus include addressing security challenges, preserving user privacy, and establishing standardized protocols and practices to ensure seamless integration and operation within the IoV ecosystem.

The progression of the Internet of Vehicles (IoV) has instigated extensive research, particularly in the realm of security. The Internet of Vehicles (IoV) faces a range of security challenges. Security attacks possess the potential to disrupt communications, jeopardize network integrity, and induce misguided decisions among connected vehicles. Researchers have categorized these attacks based on parameters such as the number of attackers and the type of malicious activity. Effectively mitigating these threats and designing strong security mechanisms are crucial to maintaining the IoV reliability.

## 1.2 Definition of IoV

IoV serves as the foundational element of the Intelligent Transport System (ITS), representing a specialized category within the realm of ad hoc networks characterized by their dynamic topology and sporadic connections, as documented in [6]. The architecture of a connected vehicle comprises three core elements : the On-Board Unit (OBU), a Road-Side Unit (RSU) or Basic Station (BS), visually depicted in Figure 1.1, and an Application Unit (AU). IoV accommodates a wide spectrum of applications, encompassing both safety-related functionalities such as lane changing assistance and non-safety applications like infotainment services.

#### 1.2.0.1 Characteristics

While some vehicular services have been successfully deployed in the IoV, the practical implementation of IoV still needs to improve, particularly in management and deployment. These difficulties arise due to several intrinsic characteristics of Vehicular Networks, such as limited scalability, relatively low intelligence, and sometimes inadequate connectivity. One of the critical challenges stems from the high dynamicity of the network topology within Vehicular Networks. Unlike traditional communication networks, Vehicular Networks are characterized by a constantly changing network topology. Vehicles move rapidly, join and leave the network, and form ad-hoc connections. This dynamicity poses a substantial challenge for effectively managing the data and control planes. The dynamic nature of Vehicular Networks is further exacerbated by the increasing number of mobile nodes, as more vehicles become equipped with communication capabilities. This exponential growth in the number of mobile nodes, combined with their mobility, creates a highly dynamic and complex network environment. Consequently, it becomes increasingly challenging to orchestrate and control the flow of data and management commands within the network. Additionally, the sheer scale of Vehicular Networks can be overwhelming, especially in densely populated urban areas, such as city centers, highways, and at the entrances to large cities. In these locations, the network encompasses a large number of vehicles, all of which may seek to access and share data simultaneously. The management of such a large-scale network requires robust solutions that can efficiently handle the high demand for resources and information dissemination. Addressing these challenges is imperative for the successful deployment and sustained performance of services within the broader framework of the Internet of Vehicles. Research and development efforts are ongoing to devise intelligent algorithms, dynamic routing protocols, and efficient resource management strategies capable of adapting to the unique characteristics of Vehicular Networks. These solutions aim to optimize the network's performance, enhance scalability, and ensure reliable connectivity, ultimately enabling the IoV

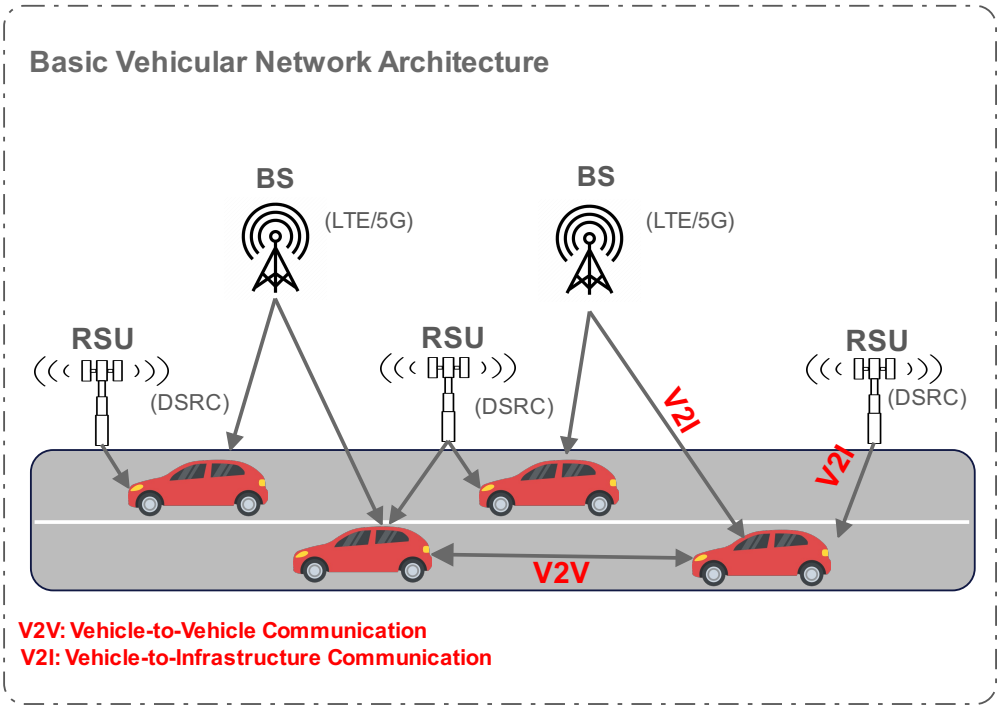



FIGURE 1.1 – Basic Vehicular Network Architecture.

to fulfill its potential in terms of improved traffic management, road safety, and a range of innovative applications. Thus, the inherent characteristics of vehicular networks, marked by high network dynamism and a burgeoning count of mobile nodes, pose significant challenges in terms of network management and deployment. Addressing these challenges effectively is pivotal to unlocking the full potential of the Internet of Vehicles (IoV) in enhancing our transportation systems and ensuring the ongoing evolution of vehicular communication networks.

While some services have already been deployed, IoV grapples with numerous difficulties in management and deployment due to factors such as limited scalability, diminished intelligence, and suboptimal connectivity. The challenges highlighted above are formidable due to connected vehicles' distinctive features, including the topology's dynamicity and the increasing number of mobile nodes. Furthermore, the sheer scale of the network, especially in densely populated urban areas like city centers, highways, and entrances to large cities, exacerbates the intricacies associated with deploying the IoV.

#### 1.2.0.2 Applications

The Internet of Vehicles (IoV) stands as a fundamental and essential element within contemporary smart city ecosystems. Fueled by a diverse range of applications, IoV significantly elevates the quality of life, enhances safety, and reinforces overall urban security. Its versatile applications cover a wide array of domains, playing a crucial role in reshaping our interactions with and navigation through urban environments.

One of the fundamental pillars of IoV is its role in ensuring urban safety. Safety applications within IoV are instrumental in averting accidents and reducing the risk to both vehicle occupants and pedestrians. For instance, blind spot warnings employ advanced sensors and real-time data exchange to provide drivers with crucial information about vehicles or obstacles in their blind spots, thereby mitigating the potential for dangerous collisions. Equally vital are IoV applications that detect traffic light violations, ensuring that drivers adhere to traffic rules and, in turn, curbing reckless driving behaviors. The synergy between IoV and safety applications is a testament to its invaluable contribution in safeguarding lives on the city's bustling streets.

Furthermore, the IoV landscape extends its reach to offer entertainment services that cater to the preferences and diversions of the modern urban dweller. The ability to stream media seamlessly within the vehicle, be it music, video content, or other forms of entertainment, adds a new dimension to the commuting experience. Passengers can access their favorite media, transforming mundane journeys into engaging and enjoyable experiences. These entertainment applications not only contribute to passengers'

comfort but also align with the broader goal of enhancing the overall quality of urban life. The convenience factor within IoV is equally compelling. In a world characterized by urban congestion and limited parking spaces, IoV applications come to the rescue by enabling parking space identification. Advanced parking management systems, integrated with IoV technology, allow drivers to effortlessly locate available parking spaces in crowded city centers, reducing the time and stress associated with finding a suitable parking spot. This, in turn, contributes to a more streamlined and efficient urban transportation system. Hence, the Internet of Vehicles represents a pivotal element of smart city environments, offering a diverse range of applications that touch upon safety, entertainment, and convenience. From averting accidents through blind spot warnings and traffic light violation detection to enhancing the quality of urban life with in-vehicle entertainment and simplifying parking through space identification, IoV's multifaceted contributions not only make cities safer but also elevate the overall urban experience. The synergy between IoV and smart city initiatives continues to redefine our urban landscapes, making them more connected, secure, and enjoyable.

### 1.2.1 Architecture's Components

In this subsection, we illustrate the communication entities and types of IoV.

#### 1.2.1.1 Communication entities

**The On Board Unit (OBU)** AAn On-Board Unit (OBU) within connected vehicles is a compact electronic device or module installed in the vehicle. OBUs are responsible for facilitating and supporting various wireless communication capabilities, processing data, and enabling interactions such as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-cloud (V2C). These units are essential components of the Internet of Vehicles (IoV) ecosystem, enabling vehicles to communicate with each other and network components, ultimately contributing to improved safety, traffic efficiency, and the overall driver experience.

**The Road Side Unit (RSU)** The Roadside Units (RSUs) are infrastructure components strategically placed along roadways. They are critical in enhancing ITS safety, efficiency, and functionality. ), designed to facilitate communication between vehicles and infrastructure elements, such as RSUs, to improve road safety traffic management and provide various value-added services to drivers and passengers. These units have various communication technologies, including wireless transceivers and sensors. It utilizes Dedicated Short-Range Communication (DSRC) based on IEEE 802.11p. It enables them to establish reliable and low-latency connections with nearby vehicles. RSUs serve as communication hubs that bridge the gap between vehicles and central traffic management systems, thus creating an interconnected and responsive network. Hence, RSU is an essential communication hub with wireless transceivers and sensors facilitating dependable and low-latency connections between vehicles and surrounding infrastructure. They bolster road safety through real-time applications like collision avoidance, lane change warnings, and emergency vehicle alerts, providing critical information to avert accidents. RSUs further contribute to efficient traffic management by delivering real-time data on traffic congestion, accidents, road closures, and signal optimization, thereby reducing congestion and improving traffic flow. Moreover, RSUs gather invaluable urban planning data on traffic patterns, vehicle density, and road conditions, supporting informed city planning and infrastructure development decisions. These units establish connectivity with diverse infrastructure elements like traffic lights, surveillance cameras, and weather stations, promoting a comprehensive smart transportation ecosystem. RSUs optimize network resources to efficiently manage data transmission and network handovers efficiently, ensuring minimal latency and reliable communication. Finally, RSUs are essential in safeguarding data security and privacy, employing authentication and encryption mechanisms to prevent malicious attacks.

**The Application Unit (AU)** The final unit in the system is the Application Unit (AU), serving as an on-board device within the vehicle. This unit establishes communication with the network through the On-Board Unit (OBU), utilizing either wired or wireless connections. Its primary function is to offer internet connectivity to other OBUs in the network.

**The Basic Station (BS)** The BSs and RSUs are running OpenFlow. They do not only carry voice calls, but they also exchanged data between the connected vehicles with each others and with the other components.

#### 1.2.1.2 Communications types

Enhancing road safety remains a formidable challenge within the domain of Intelligent Transportation Systems (ITS). In this pursuit, considerable research efforts have been directed towards the improvement of communication systems in vehicular networks. Reducing accidents continues to be a complex endeavor for connected vehicles, which play a pivotal role in elevating the driving experience and traffic management. Their mission is to establish robust, secure, safe, available, and scalable connections between vehicles and various communication entities through the vehicle-to-everything (V2X) communication types as illustrated in Figure 1.2.

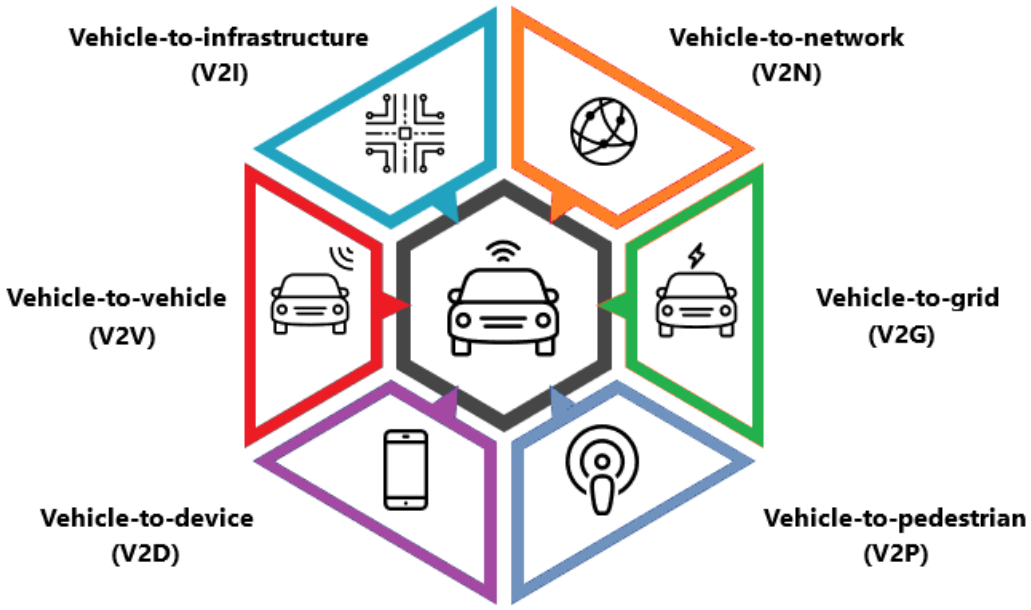



FIGURE 1.2 – Vehicle-to-everything (V2X) communications types in IoV.

V2X serves as the foundation for essential services like road safety and collision warnings, as well as in-vehicle internet connectivity. Consequently, a multitude of services are poised to be delivered by connected vehicles, ranging from real-time traffic alerts and route planning to cloud-based offerings.

Among the various V2X sub-types, V2V and V2I emerge as particularly influential, profoundly reshaping the driving experience. However, the successful implementation of these technologies necessitates a significant shift in connectivity infrastructure. The seamless provision of broadband is indispensable for the operation of these advanced mesh networks.

To confront this challenge, various industry groups have directed their efforts towards transitioning from the older radio technology, based on the 802.11p standard, utilized for V2X communications, to a cellular standard known as Cellular Vehicle-to-Everything (C-V2X). C-V2X integrates cellular network communication with direct interactions between vehicles, infrastructure, and other road users. It capitalizes on the extensive coverage provided by established 4G/LTE networks, with future adaptability expected for 5G and 6G networks, presenting a more comprehensive set of capabilities compared to other vehicle connectivity solutions. In contrast to the short-range communications of 802.11p, which necessitate multiple network hops to gather information about traffic conditions a mile ahead and rely on numerous vehicles or nodes, C-V2X facilitates real-time, single-step communication. This long-range communication capability enhances the ability to predict traffic conditions and lays the groundwork for more precise and effective traffic management.

C-V2X has undergone extensive testing in collaboration with numerous automobile manufacturers, maturing over the years before gaining definitive validation. Simultaneously, the 5G and 6G networks have continued their expansion, with the United States set to provide widespread coverage along major highways by 2025.

While C-V2X is still considered a relatively recent technology, V2X is already contributing to safer driving. The ensuing sections provide a detailed exploration of each V2X communication type.

**Vehicle-to-Infrastructure (V2I)** This signifies the interaction between vehicles and other communication entities (e.g., RSU, BS). In this context, vehicles transmit essential parameters such as their

position, speed, direction, and more, which are crucial for various applications, including video streaming. The RSUs play a pivotal role in collecting and processing these transmitted parameters, enabling the provision of necessary services.

Simultaneously, Vehicle-to-Infrastructure (V2I) communication empowers vehicles to establish connections with stationary infrastructure components, such as traffic lights, which are integrated as nodes within the mesh network. This interaction brings about significant enhancements in various aspects of traffic management. It contributes to improved traffic safety through the delivery of warnings for potentially hazardous situations, facilitates intersection optimization, and ensures the safe operation of rail crossings. Furthermore, V2I aids in mitigating traffic congestion by providing real-time notifications of traffic jams, enabling dynamic traffic light control, and offering assistance in finding available parking spaces. Additionally, V2I contributes to the reduction of emissions and air pollution, aligning with the broader goals of sustainable and environmentally friendly transportation solutions.

**Vehicle-to-Vehicle (V2V)** This sub-type of communication, as discussed in prior research [7], introduces novel applications, notably safety and infotainment services [8], which have the potential to significantly enhance overall safety on the roads. This is particularly crucial given the staggering number of global fatalities resulting from motor vehicle accidents. Alternatively, when a direct connection is not available, such as in cases of longer-distance communication, routing protocols are employed, known as k-hop communication. These routing protocols encompass various strategies, including clustering-based approaches [9][10], route-discovery methods, or broadcasting protocols [11]. V2V communications are instrumental in sharing critical data concerning factors like speed, direction, position, and braking status with neighboring vehicles. In essence, this facilitates the creation of a mesh network among vehicles, with each vehicle transmitting, receiving, and re-transmitting messages to others within an approximate range of 300 meters. Additionally, it is important to note the existence of an Intra-Vehicle communication class within the V2V domain.

**Vehicle-to-Pedestrian (V2P)** This sub-type symbolizes communications with nearby wheelchairs and bicycles of person.

**Vehicle-to-Grid (V2G)** This facet of communication involves the exchange of data with the smart grid, aimed at achieving more efficient load balancing. It encompasses two distinct sub-categories : communicationg of vehicles with building, home, and load.

**Vehicle-to-Device (V2D)** This category involves the exchange of data between a vehicle and various electronic devices that can connect to the vehicle via Bluetooth or WiFi-Direct, including systems.

**Vehicle-to-Network (V2N)** This category represents communication based on Cellular (3GPP) / 802.11p technology. It comprises four distinct sub-categories : Vehicle-to-Cloud (V2C) (e.g., remote vehicle diagnostics using DoIP) and Vehicle-to-Pedestrian (V2P) (e.g., involving wheelchairs and bicycles). It's worth noting that V2I, V2V, and V2P are also considered sub-categories within V2N.

## 1.3 Software-Defined Networking Based IoV

### 1.3.1 Software-Defined Networking (SDN)

The core principle of SDN revolves around separating the control and data plane [13]. In this architecture, the SDN Controller (SDNC) resides in the control plane and monitors, manages, and optimizes networking resources. Its primary goal is improving network performance, traffic control, and efficient communication. Meanwhile, the data plane encompasses the networking infrastructure, including forwarding devices and wired/wireless links. SDN introduces the flexibility to design a programmable networking framework, with OpenFlow (OF) being the most widely used interface. OF facilitates communication between both planes, bridging the control and data realms. Another component, the application plane, involves third-party services and applications. Through an application-control interface, the SDN Controller manages the requirements of SDN applications, covering aspects like security, Quality of Service (QoS), and resource allocation. SDN provides two types of interfaces for this purpose : the Control-Data Plane Interface, known as the southbound Interface API (e.g., OpenFlow), and the Application-Control Plane Interface, called the northbound API (e.g., REST API). The primary objectives of SDN include enhancing network security, simplifying network management, supporting network heterogeneity, and optimizing resource utilization through OpenFlow. This entails the SDN Controller communicating with OF-Switches

to gather essential information. Using various anomaly-detection tools and traffic analyses, OF-Switches collect the necessary data. The SDNC then analyzes this information, allowing for creating or modifying network configurations and implementing new policies or rules to address potential security issues. This proactive approach enables swift control over identified security vulnerabilities.

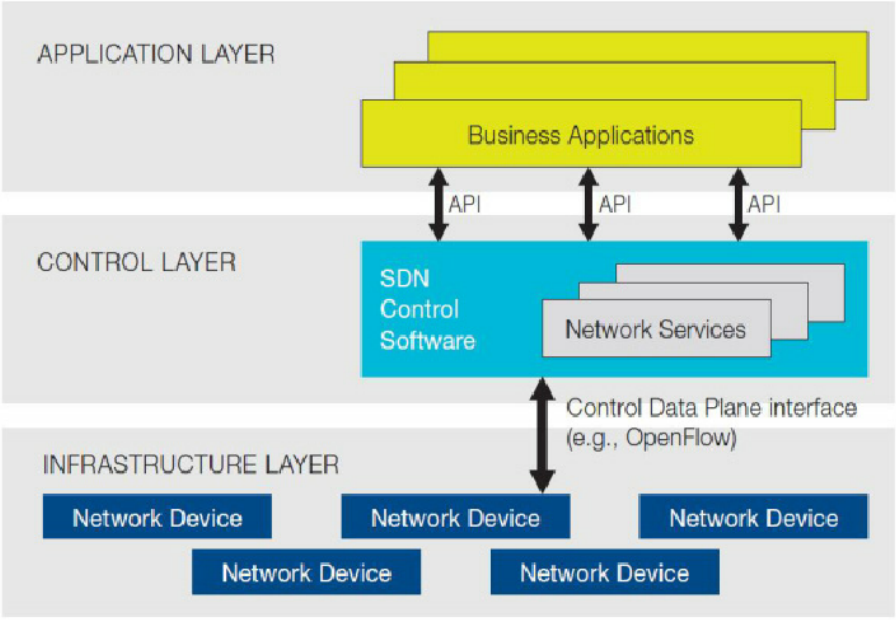



FIGURE 1.3 – SDN architecture.

### 1.3.2 Software-Defined Vehicular Network (SDVN)

In alignment with the core vision of our work, which revolves around proposing a secure hierarchical vehicular network architecture aimed at significantly enhancing its security services, we advocate the adoption of the Software-Defined Networking (SDN) paradigm as the foundational framework for our architecture as illustrated in Figure 1.4. Beyond the benefits of this hybrid approach, we harness the inherent advantages of the SDN paradigm to streamline management processes and bolster control.

SDN-based vehicular networks play a pivotal role in advancing 5G technology. These networks facilitate diverse services by enabling communication among vehicles and the entities outlined in subsection 1.2.1.1. Intelligent Transportation Systems (ITS) have introduced this emerging technology to provide drivers with enhanced comfort, safety, and infotainment services while improving traffic efficiency. In contrast to traditional vehicular networks, which often grapple with managing dynamic and large-scale networks constrained by fixed policies and complex architectures, SDN introduces a transformative aspect. It establishes logical and centralized control across the entire network, making vehicular networks flexible and programmable, ready to accommodate new services and features.

The centralized controller in the control plane takes charge of orchestrating network functionalities and packet forwarding through devices in the data plane. This SDN-based approach enhances the efficiency of the Internet of Vehicles (IoV) and strengthens security measures for connected vehicles. However, it is crucial to acknowledge that integrating new technologies and architectural components in the network also introduces new security challenges that require attention and resolution.

#### 1.3.2.1 Hierarchical Control Plan

The decision to implement a hierarchical structure for the control plane is underpinned by the overarching vision of our work, which emphasizes the need for unified control in these networks. At the second level, the controller is tasked with constructing a comprehensive view of the communication infrastructure. This view is established by aggregating information provided by each network's local controller. The second-level controller defines and disseminates global rules that delineate the overarching behavior of the entire network. In contrast, the first-level local controllers, which oversee the Basic Stations (BS) and Road-Side Units (RSU), formulate specific rules for individual network nodes. It's worth noting that certain network control decisions can be autonomously made by the local controllers without explicit directives from the global controller. For instance, decisions pertaining to horizontal handover operations

(altering the attachment point within the same network, such as switching from one BS to another) can be locally managed.

Conversely, vertical handover operations, which involve transitioning between different network entities (e.g., switching from an RSU network to a BS network), may necessitate guidance from the global controller. In the subsequent sections, we provide examples of network control functions at each level of control. While local controllers can typically be associated with the entities responsible for each specific network, the role and responsibilities of the second-level global controller remain a subject of consideration.

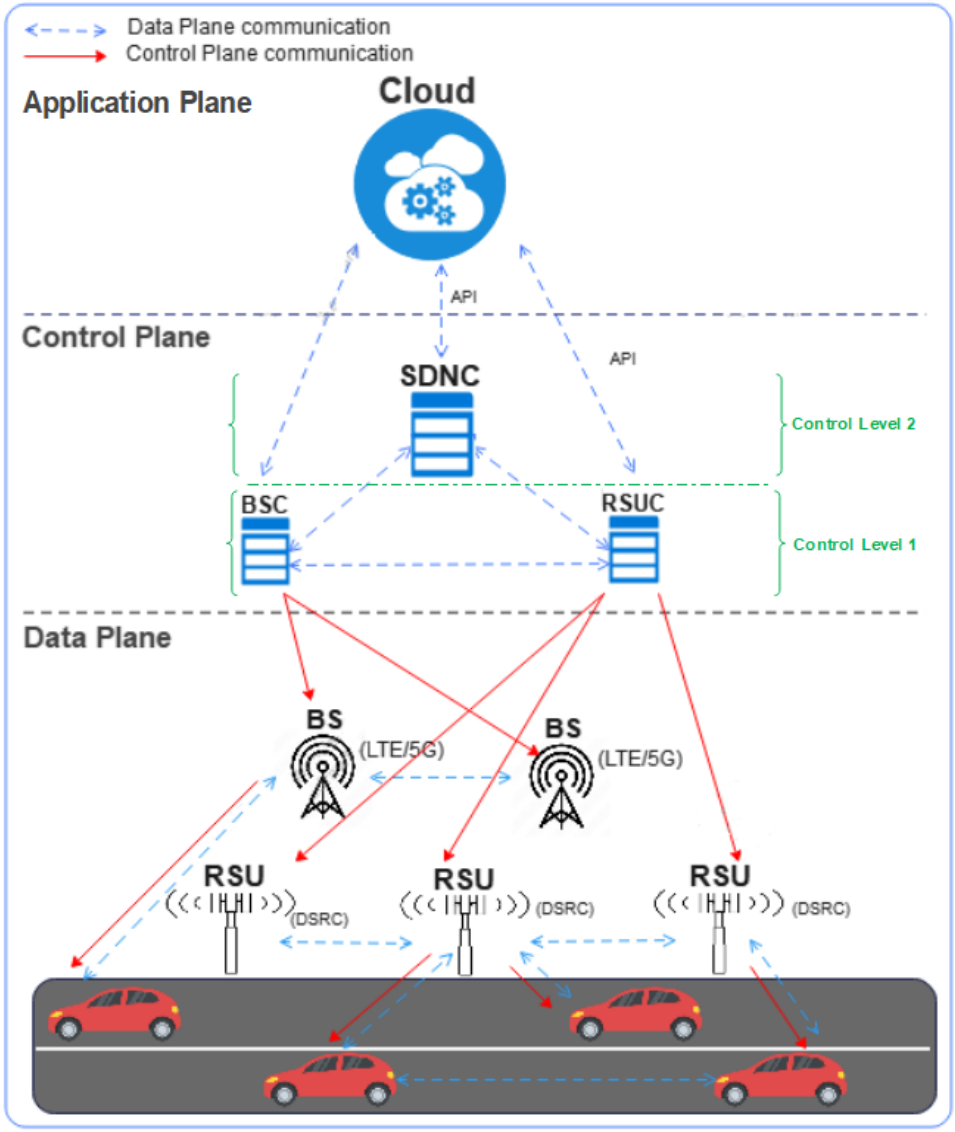



FIGURE 1.4 – Proposed hierarchical SDN-based Vehicular Network (SDVN) architecture.

## 1.4 Security and privacy for IoV

Before deploying any IoV, great attention to security and privacy concerns must be taken into account. Hence, users' privacy-preserving and securing the network and transmitted data from entities with malicious intent is still a challenging task in the IoV context, especially with integrating new technologies into the architecture. Besides taking advantage of integrating new architectural components and paradigms into the architecture, this exposes new security vulnerabilities to the IoV.
We explain more in details the security concerns in IoV and the privacy-preserving in the two following subsections.

### 1.4.1 Security requirements in IoV

Security in vehicular networks is of paramount importance as it directly impacts safety in potentially hazardous situations. Ensuring the integrity of critical data is vital, especially when there's a risk of malicious alterations. In the realm of the Internet of Vehicles (IoV), the challenge lies in striking a balance between managing a driver's responsibilities and safeguarding their security. This task is complex due to various factors such as network scale, vehicle speeds, geographic coverage, and the dynamic nature of vehicular associations. In-vehicle systems offer significant computing and power resources, setting them apart from typical systems. These systems are capable of processing extensive amounts of data, often involving multiple chips. Malicious actors can be categorized along three dimensions : "inside and outside the network," "illegitimate and legitimate actors," and "active and passive threats." Message-based attacks can manifest in various forms, including "misinformation," "location information fraud," "identity exposure," "denial of service," and "concealment." The collection and sharing of data within vehicular networks raise concerns about data integrity. For example, a sender might manipulate information to gain an advantage (e.g., falsely reporting traffic congestion to divert other vehicles onto less crowded routes). Malicious entities often pose as different vehicles or road infrastructure, creating security risks. Establishing a trust system and recognizing vulnerabilities from senders can help vehicles mitigate this risk.

### 1.4.2 Privacy requirements in IoV

Preserving privacy is a critical concern within the context of vehicular networks. This is primarily due to the inherent link between a connected vehicle's identification and location information with a user's actual identity and other sensitive data. Malicious actors can exploit this connection to determine a vehicle's location using its identification and to track its trajectory over time. To counter this threat, it's advisable to replace real identities with pseudonyms, and changing these pseudonyms regularly can help prevent tracking.

Considering the privacy challenges mentioned earlier, adopting privacy-preserving authentication schemes becomes crucial in connected vehicles. In this context, conditional privacy-preserving implies that only the Trusted Authority (TA) can reveal a connected vehicle's real identity through the messages it receives.

Key privacy-preserving requirements in vehicular networks include :

- **Privacy and anonymity :** In the realm of the Internet of Vehicles (IoV), it's imperative that vehicular devices do not disclose the personal, confidential, or private data of their users. The activities of one vehicle should remain concealed from others, and the concept of anonymity might only be relevant or necessary for specific vehicles within the IoV.
- **Message authentication and integrity :**Communication through messages in the IoV should be safeguarded to prevent any unauthorized modifications, and the recipient of a message must be able to prove the sender's identity. It is important to note that ensuring message integrity does not necessarily mean establishing the identity of the data sender.

- **Message non-repudiation :**Message non-repudiation in vehicular networks is a crucial concept that ensures a sender cannot deny sending a specific message, and a recipient cannot deny receiving it. This concept plays a significant role in ensuring trust and accountability within the Internet of Vehicles (IoV). To achieve message non-repudiation in IoV, various security measures are employed, including cryptographic techniques, secure timestamps, and message logging. These measures collectively guarantee that both senders and recipients cannot deny their roles in the exchange of messages. This is vital for maintaining the reliability and security of vehicular communication systems.

- **Entity authentication :** Authentication is a pivotal aspect of security, and it has a significant impact on privacy concerns within the context of vehicular networks. Authentication not only ensures that the sender created a message but also provides evidence of the sender's identity. This verification is crucial for confirming the legitimacy of vehicles, infrastructure components, and other communication nodes, preventing impersonation, and facilitating secure and dependable communications in Vehicular networks. In some authentication protocols in the Internet of Vehicles (IoV), mechanisms are implemented that allow entities to prove their authenticity without disclosing their actual identity. This approach strikes a balance between security and privacy, which is essential in IoV systems.

— **Access Control :** Access control and privacy-preserving mechanisms play a critical role in Vehicular networks by striking a balance between the necessity to communicate information for safety and traffic management and the imperative to safeguard the privacy of users and their connected vehicles. These mechanisms ensure that only authorized entities can access specific information while also preserving the anonymity of all participants, addressing the twin goals of controlled access and privacy protection in Vehicular networks.

— **Message confidentiality :**Vehicular networks frequently involve vehicles sharing information regarding their location and activities. Message confidentiality pertains to safeguarding the content of messages shared between connected vehicles and infrastructure, ensuring that they are shielded from unauthorized access or eavesdropping. By upholding message confidentiality, the privacy of drivers is preserved, as it ensures that message details, including sensitive location and identity information, are secure during communication and remain protected from unauthorized or malicious entities.

### 1.4.3 Balance between Security and Privacy

This subsection addresses the delicate balance between security and privacy, recognizing that striking the proper equilibrium is paramount. We delve into the balance between privacy and security in vehicular networks from three perspectives.

Firstly, the implementation of authentication schemes may raise privacy concerns as sensitive location information is exposed to the Trusted Authority (TA) at a particular time. While such schemes enhance security, some users might resist the notion of being under the TA's surveillance, as it appears to infringe upon their privacy.

Secondly, it is worth noting that augmenting security often comes at the cost of increased privacy concerns, particularly when privacy protocols are employed.

Thirdly, the Certificate Revocation List (CRL) has traditionally been employed to blacklist malicious nodes. However, this approach demands significant storage space due to the scale of Vehicular networks. In response, researchers have proposed alternative revocation mechanisms that utilize storage strategies and hashing techniques to make neutral services more accessible. Nevertheless, it's essential to recognize that checking a certificate's status in these mechanisms may inadvertently reveal the user's private information, a departure from the traditional CRL method.

## 1.5 Conclusion

The primary goal of IoV research is to improve the driving experience by focusing on safety, security, and the conditional protection of drivers' true identities and private information within vehicular networks. These networks come with a set of complex challenges, mainly due to their interconnectedness with other rapidly expanding domains. Security and privacy preservation stand out as the most crucial concerns, necessitating further research and development efforts to elevate the quality of service and security within IoV, all while addressing the unique challenges it presents.

In this chapter, we have discussed a general view of IoV by defining its primary pillars : characteristics, applications domains, architecture's components. We also discussed the importance of integrating the SDN paradigm in the IoV context. We illustrated the proposed architecture of SDN-based vehicular network (SDVN). A comprehensive description has been presented to explain our choice to present hierarchically the control plane in the SDVN architecture. Then, we delved into the security and privacy requirements specific to the IoV.

CHAPITRE 2

# VEHICULAR NETWORKS' TRUST MANAGEMENT

## Table des matières


2.1 Introduction . . . 30
2.1.1 Contributions of this work . . . 30
2.1.2 Structure of the chapter . . . 30
2.1.3 Research Methodology . . . 34
2.2 Overview of Trust Management Mechanisms . . . 35
2.2.1 Characteristics . . . 35
2.2.2 Metrics . . . 36
2.2.3 Computation modules . . . 36
2.3 Existing Surveys . . . 37
2.3.1 Contributions of existing surveys . . . 37
2.3.2 Comparison with our work . . . 37
2.4 Issues . . . 38
2.4.1 Security Issues . . . 38
2.4.2 Trust management Issues . . . 38
2.4.3 Security attacks in IoV. . . . 39
2.5 Classification . . . 41
2.5.1 Entity-based schemes . . . 41
2.5.2 Hybrid schemes . . . 43
2.5.3 Technology-based classification . . . 44
2.6 Discussion . . . 49
2.6.1 Summary . . . 49
2.6.2 Comparison . . . 49
2.7 Future Work . . . 54
2.7.1 Federated Learning-based solutions . . . 54
2.7.2 Clustering approaches . . . 54
2.7.3 Energy consumption . . . 54
2.7.4 Emerging technologies . . . 55
2.8 Conclusion . . . 55

## 2.1 Introduction

The data transmission in the IoV [15], occurs within an open-access environment, and security and privacy emerge as pivotal concerns associated with Vehicular networks. Consequently, any IoV-based system should meet the security and privacy prerequisites [22] outlined in Tables 2.1 and 2.2 to ensure an efficient and dependable system. It is imperative to ensure that the messages being exchanged remain untampered and free from any unauthorized alterations by potential threats such as insider or outsider attackers, malicious or rational actors, and local or extended adversaries. The compromise of applications within the Internet of Vehicles (IoV) can pose significant threats to drivers and passengers. Citing data from the World Health Organization [23], it is reported that over 1.35 million road users lose their lives annually in accidents. Consequently, ensuring authentication and trust [24] in extensive data exchange becomes an indispensable necessity in the realm of IoV. The significance of privacy in connected vehicles cannot be overstated. Consequently, only Trusted Authorities (TAs) [25] are granted access to sensitive and private vehicle-related information. This access is essential to safeguard drivers' privacy from any third-party intrusion and maintain accountability. Therefore, Trusted Authorities (TAs) play a crucial role in tracking malicious nodes and revealing their identities when these nodes propagate false information regarding vehicle position or traffic conditions within the network. The messages exchanged often contain personal driver information and must be sent anonymously to ensure communication efficiency. However, additional measures are essential to guarantee the authenticity of these messages. There are instances where internal nodes may disseminate false messages across the network, potentially leading to catastrophic accidents. If Trusted Authorities (TAs) and Roadside Units (RSUs) identify such false messages, they must uncover and disclose the actual identity of the malicious node responsible for spreading misinformation.

The primary role of TAs involves registering participant vehicles and RSUs, generating their private keys, and establishing security parameters [26]. Additionally, TAs assign pseudo-identities to registered vehicles while retaining their real identities for tracing any malicious activities. RSUs are responsible for scrutinizing messages from vehicles to thwart deceptive information attacks, requiring the ability to detect false information reports originating from vehicles. As a result, establishing a Public Key Infrastructure (PKI) becomes a critical necessity in Vehicular networks. Many security solutions rely on traditional PKI, which excels at promptly identifying outsider attackers but needs to catch up in detecting insider attackers already network participants with validated credentials [27]. Consequently, researchers introduced the concept of trust [28] as a security parameter capable of uncovering insider attackers by scrutinizing mutual messages.

Furthermore, trust-based approaches are still in the early stages of development to ensure the effectiveness of IoV deployment. Under trust models, nodes assign trust levels to one another during communication within the network. Trust management has garnered significant attention from researchers [29] due to its potential to disseminate reliable information, eliminate false messages, track self-serving and malicious nodes, and mitigate their activities. Therefore, implementing trust models in RSUs and vehicles becomes imperative to gauge received messages' reliability, accuracy, and authenticity.

### 2.1.1 Contributions of this work

This chapter offers an extensive examination of trust management within the realm of connected vehicles. Despite the growing interest from contemporary researchers in the implementation of trust mechanisms in these networks, there remains a scarcity of comprehensive surveys explicitly focused on this subject matter. Consequently, in this survey, we undertake a thorough review, analysis, and comparative evaluation of the various trust management schemes introduced within the past six years, covering the period from 2017 to 2022, all of which have been developed to address trust management in the IoV.

Furthermore, we categorize these schemes based on their alignment with emerging technologies and the utilization of Artificial Intelligence tools. The structure and organization of our survey are visually depicted in Figure 2.1.

### 2.1.2 Structure of the chapter

In section 2.2 of this chapter, we provide a comprehensive overview of the trust management mechanism in connected vehicles. Section 2.3 delves into existing survey papers on this subject. In Section 2.4, we recap the security and trust management challenges, along with the most prevalent attacks in Vehicular networks. Section 2.5 presents a fresh classification of these approaches based on the technology employed. Section 2.6 summarizes the surveyed trust management approaches in IoV and provides

TABLE 2.1 – **Security services in IoV.**

| Service | Description |
|---|---|
| Availability | Availability is indeed a fundamental aspect of security. Ensuring the availability of resources, such as network services, is critical because many attacks aim to disrupt or deny access to these resources, which can have significant consequences. By maintaining high availability, a network can resist various types of attacks and continue to provide services to its users, contributing to a more secure and reliable environment. |
| Authentication | Authentication is essential in network security to verify the legitimacy of nodes or users accessing a network. Authentication mechanisms ensure that users or devices are who they claim to be before granting access to network resources. This helps prevent unauthorized access and unauthorized actions within the network, enhancing security and trust. |
| Data integrity | Message integrity ensures that data transmitted within a network remains unchanged during transit and reaches the recipient in the same state as originally sent by the legitimate user. This protection against unauthorized modification or tampering is vital for maintaining the trustworthiness and reliability of the information exchanged in the network. Strong message integrity mechanisms help prevent attackers from altering data and ensure the authenticity and accuracy of the information. |
| Confidentiality | Message confidentiality is a security service that focuses on preserving the privacy of users by encrypting the contents of messages exchanged between communicating nodes. It ensures that unauthorized entities cannot access or understand the information being transmitted. By encrypting data, the contents remain confidential, and only authorized recipients with the decryption keys can access and interpret the data, thus protecting the user's privacy. |
| Non-repudiation | Message non-repudiation is a security service designed to ensure that both the sender and receiver of messages cannot deny having sent or received specific messages. This service enhances accountability and prevents parties from disavowing their involvement in the exchange of messages, thereby fostering trust and reliability in communications. |

TABLE 2.2 – **Privacy requirements in the IoV.**

| **Requirement** | **Description** |
|---|---|
| Availability | Ensuring the availability of resources is a critical requirement in IoV, especially since many attacks target the availability of these resources. It's essential to maintain a reliable and stable network to support the safety and functionality of vehicular communication systems. |
| Data Authentication | Ensuring the integrity and authenticity of exchanged information between IoV entities is crucial. Verification of transferred data is instrumental in preventing tampering and unauthorized access, thereby bolstering the overall security of vehicular communication systems. |
| Integrity of data | This requirement is about ensuring that transmitted messages reach their intended destinations without being intercepted or redirected by unauthorized entities. It helps maintain the integrity and reliability of communication in vehicular networks. |
| Privacy of vehicle | This requirement emphasizes the need to protect users' personal and confidential data, as well as ensuring the security of transmitted messages and preventing unauthorized entities from accessing information about the future activities of network nodes. It emphasizes the significance of privacy and security within vehicular networks. |
| Authorization | This requirement ensures that only authorized entities within the Internet of Vehicles (IoV) can access and benefit from the services provided by the network, enhancing security and control over network resources. |
| Vehicles ID tracking | This requirement emphasizes the ability of the network to track and verify the identity of vehicles, which is crucial for security, accountability, and tracking purposes within the Internet of Vehicles (IoV). |
| Scalability | This requirement highlights the scalability of vehicular networks, allowing for the addition of new nodes without significantly impacting network performance. It's essential for accommodating the dynamic nature of vehicular environments where vehicles may join or leave the network frequently. |
| Efficiency | This requirement emphasizes the need to improve network performance by minimizing various factors, including overhead (unnecessary data or control information), computational complexity, delays in data transmission, and collisions (interference between data transmissions). These optimizations contribute to a more efficient and responsive vehicular network. |
| Freshness | This requirement stresses the importance of regularly verifying new messages in order to prevent the use of outdated or potentially compromised messages. Regular message verification helps ensure the integrity and security of the communication in vehicular networks. |

TABLE 2.3 – **Existing surveys on Vehicular networks.**

| Ref. | Year | Major contributions | Topic |
|---|---|---|---|
| [31] | 2017 | Summary of Vehicular Network Architecture, Examination of Security Concerns, Implementation of Protective Measures, and Comparative Evaluation. | Security |
| [32] | 2020 | In-depth exploration of diverse attack vectors, suggested remedies, and a thorough scrutiny and juxtaposition. | Security |
| [33] | 2019 | Survey of Vehicular Network Architecture, Deliberation on Security Threats, and Examination of Associated Challenges. | Security |
| [34] | 2021 | A comprehensive exploration of vehicular networks, attack models, and an analysis of the security and privacy requirements for identity-based security and privacy approaches. | Security, privacy |
| [35] | 2021 | A survey of vehicular networks, exploration of various attack scenarios, detailed examination of privacy and authentication schemes, countermeasures against attacks, assessment of performance metrics, and consideration of outstanding challenges. | Security, privacy |
| [36] | 2021 | Evaluation of Current Authentication and Privacy Solutions, In-Depth Comparative Analysis Using Defined Criteria, and Qualitative Assessment in Contrast to Previously Published Surveys. | Privacy |
| [37] | 2021 | This survey aims to review, interpret, and juxtapose recently introduced trust-building and management schemes, as well as to explore the shortcomings of existing research and the prospects of future challenges. | Trust |
| [38] | 2019 | Comprehensive Examination of Vehicular Networks, Scrutiny of Authentication Schemes, In-Depth Review of Location Privacy Safeguarding Approaches, Analysis of Trust Management Models, and Exploration of Future Research Directions. | Security, trust and privacy |
| [39] | 2018 | Identification and Evaluation of Contemporary Challenges in Efficient Routing Protocols, and Elaborate Qualitative Comparison. | Routing |
| [40] | 2018 | In-depth Exploration and Categorization of Pseudonym Changing Strategies, Comparative Analysis Utilizing Pertinent Criteria, Identification of Ongoing Challenges, and Consideration of Future Research Directions. | Privacy |
| [41] | 2020 | An in-depth analysis of the machine learning-based trust frameworks presently employed. | Trust |
| [42] | 2018 | Identification of Trust Management Approaches, Thorough Analysis Including Concepts, Methodology, Algorithms, Quality of Service (QoS) and Performance Characteristics, Qualitative Comparison, and Recognition of Outstanding Research Gaps. | Trust |
| [43] | 2018 | This survey focuses on Quality of Service (QoS) in the IoV and provides a quantitative comparison of various routing protocols. | QoS |
| [44] | 2019 | Comprehensive Examination of Security Attacks and Safeguarding Mechanisms. | Security |
| [45] | 2019 | Overview of Contemporary Trust Management Solutions in Vehicular Networks. | Trust |
| [46] | 2017 | Summary of Security Challenges and Examination of Authentication and Trust Models. | Security, trust |
| [47] | 2022 | Comprehensive Review : Communication Infrastructure, Applications, Identifiable Challenges, and Outstanding Concerns. | Security |

a comparative analysis using a predefined set of criteria. Section 2.7 investigates unresolved issues and potential future directions. Finally, we conclude with some closing remarks in Section 2.8.

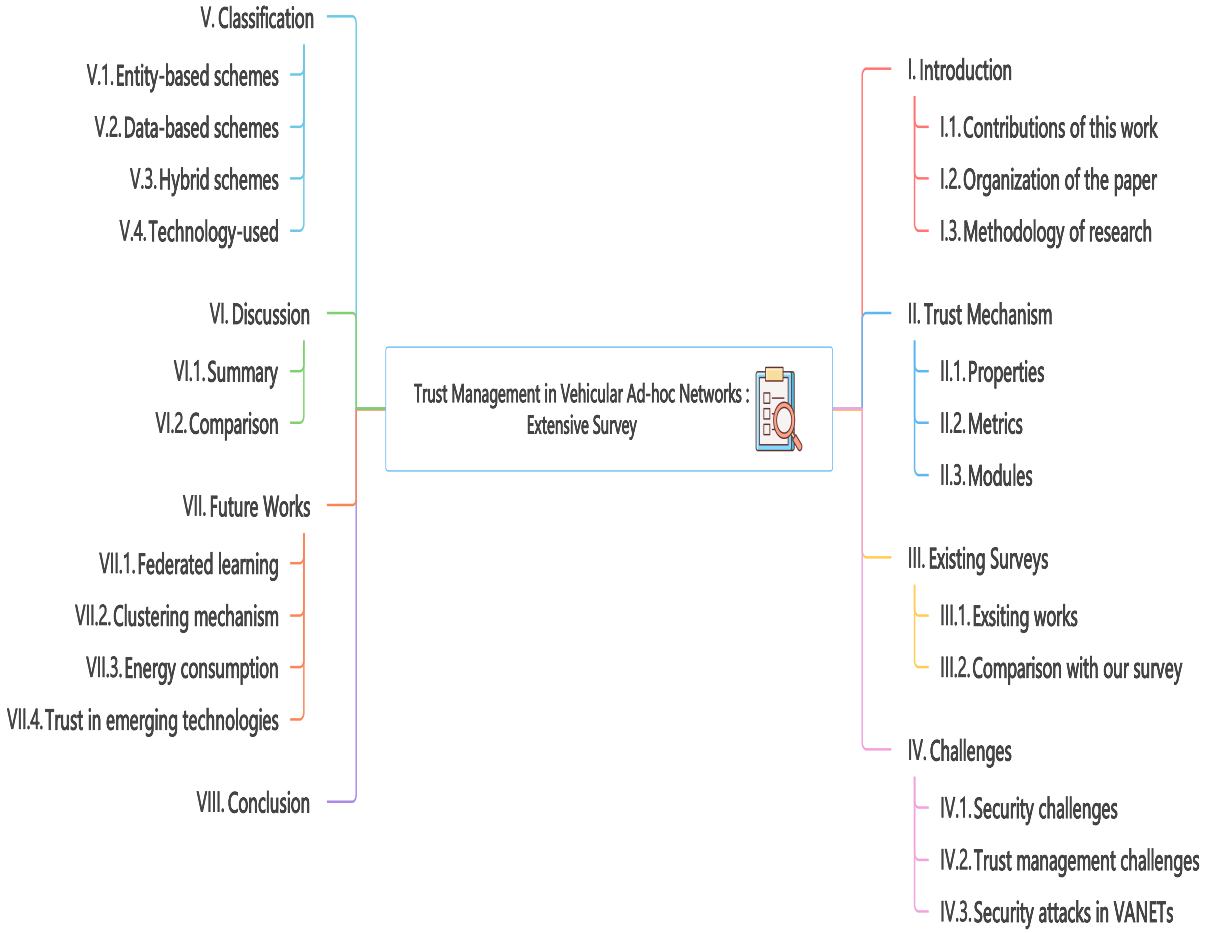



FIGURE 2.1 – Our Survey organization.

### 2.1.3 Research Methodology

This chapter aims to provide an extensive review, classification, comparison, and summary of research conducted in the domain of trust management within Vehicular Networks from 2017 to 2022. The survey is based on a selective methodology that primarily considers the year of publication and adopted tools as the search criteria. The works featured in this chapter are chosen to address specific questions, ensuring a focused and relevant discussion.

— What fundamental components constitute trust management in the context of connected vehicles ?
— Which standard metrics are commonly employed for evaluating trust within these networks ?
— What classification methods can be applied to categorize recent trust management schemes ?
— What criteria can be employed to encapsulate and summarize these approaches ?

In our search for selected surveys, we employed relevant keywords including "connected vehicles," "IoV," "Trust," and the "used tools." This yielded a substantial number of papers related to the topic. While conducting the search, it became evident that "privacy" and "reputation" are closely associated with the concept of "Trust." To further narrow down and identify more specific and recent papers, we refined our keyword criteria by combining "Trust management" and "connected vehicles" with additional terms such as "Cloud Computing," "SDN," "Edge/Fog Computing," "Blockchain," and "Artificial Intelligence techniques." This refined approach aimed to enhance the relevance and specificity of our selected surveys.

## 2.2 Overview of Trust Management Mechanisms

In general, trust pertains to the relationship between two entities in a network, which we refer to as trustors and trustees in this chapter. The trustor denotes the entity responsible for evaluating the trustee, while the trustee signifies the entity under scrutiny by the trustor. To illustrate, when X places trust in Y, X assumes the role of the trustor, and Y serves as the trustee. In this section, we explain and define the trust mechanism, which is indispensable for comprehending the surveyed approaches discussed in this chapter. Establishing secure vehicular network communications mandates the implementation of resilient and efficient trust management models. The central objective of the trust mechanism is to ascertain whether information from a sender node should be accepted or rejected by the receiving node, which can be a vehicle or an RSU, based on a specific degree of confidence denoted as the trust value. The trust value signifies the likelihood of a particular action being executed by an entity or node within the network, ranging from 0, indicating complete distrust, to 1, signifying complete trust. An overview of the fundamental principles of the trust management mechanism is presented in Figure 2.2.

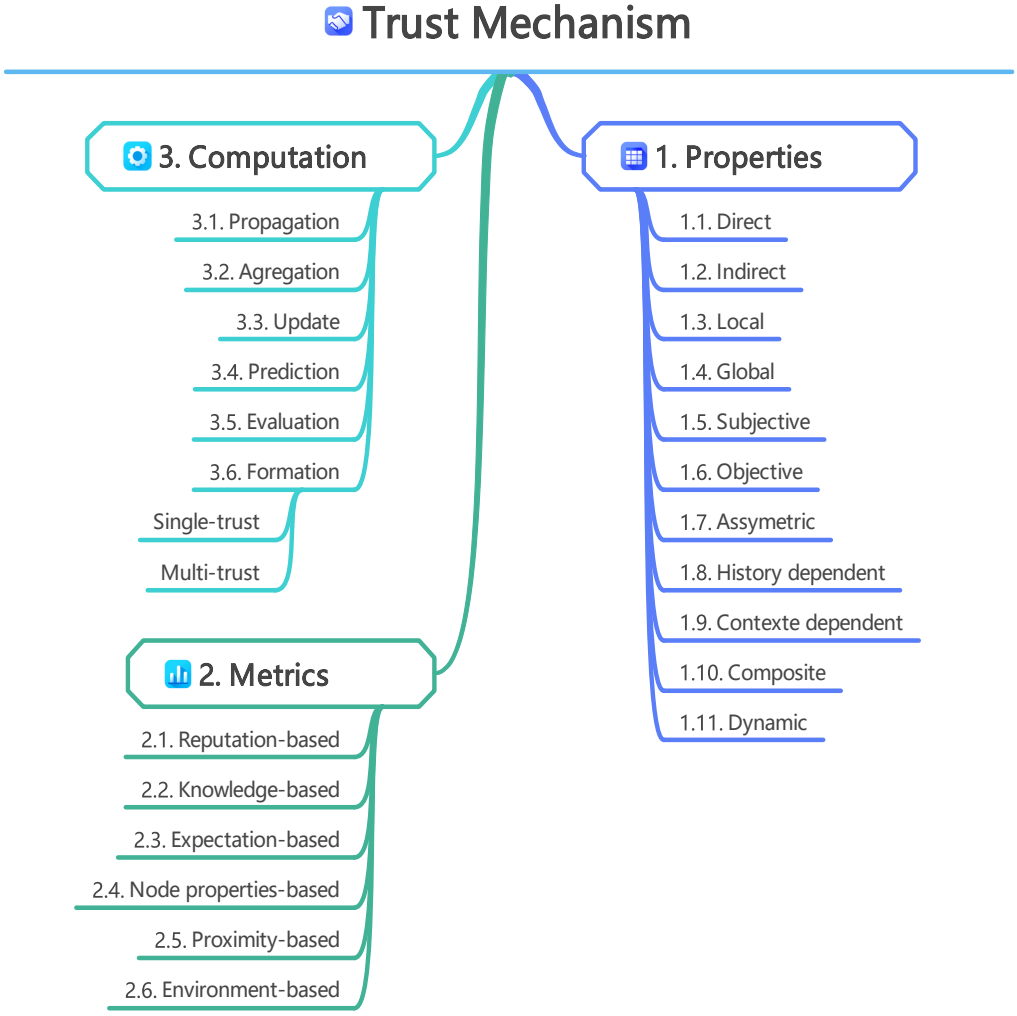



FIGURE 2.2 – Trust management main pillars.

### 2.2.1 Characteristics

The trust mechanism encompasses various properties, which can be defined as follows :

— Direct : Trust value computation relies on the immediate association between the trustor and the trustee.

— Indirect : Trust value computation depends on the endorsements disseminated by the trustor's neighboring entities.

— Local : The trust value is confined to both parties and is not disseminated within the network.

— Global : Every network entity possesses a distinct and universal trust value that is exchanged with all other entities in the network.
— Subjective : Trust calculation is solely contingent on the judgment formulated by the trustor.
— Objective : Trust calculation is contingent on specific attributes or parameters of the trustee node.
— Asymmetric : This represents a one-way or unidirectional trust relationship. For instance, if A trusts B, it does not imply automatic trust from B towards A. Asymmetric trust indicates that when A trusts B, B does not reciprocate the trust towards A.
— History-dependent : Trust calculation relies on the past behaviors and actions of the trustee.
— Context-dependent : Trust calculation is contingent on environmental events or specific circumstances.
— Composite : The trust value is computed by considering various parameters, such as honesty, security, and more.
— Dynamic : The trust value is subject to change over time and can be updated in response to alterations in the initial parameters.

### 2.2.2 Metrics

Drawing from the surveyed approaches, this section outlines the various metrics commonly employed in the measurement and evaluation of trust within Vehicular networks.

— Reputation-based : Nodes determine the trust value by considering recommendations and opinions provided by neighboring nodes in the network regarding a particular node.
— Knowledge-based : The trust calculation of a node relies on its past or direct experiences with a particular node within the network.
— Expectation-based : Trust value is calculated based on the node's anticipation or forecast of another node's behavior. In this approach, the node will compute trust either based on historical interactions with another node or predict it when there is no prior communication.
— Node properties : Trust calculation involves the key attributes of the node, such as its direction, speed, velocity, and more.
— Proximity-based : The network's trust calculation formula incorporates proximity-related parameters of the node, including factors like time, distance, location, and more.
— Environment-based : Factors such as the network area, density, or topology, including the presence of essential components like the cluster head within the clustering mechanism, are considered parameters that can be integrated into the trust formula of the system.

### 2.2.3 Computation modules

Trust management is a vital component in safeguarding communication within the Internet of Vehicles (IoV) environment. The principal modules of the trust management mechanism in Vehicular networks encompass :

— **Trust Propagation Module :** The trust propagation module employs various approaches, including distributed, semi-distributed, and centralized methods. Within the distributed approach, each individual node takes on the responsibilities of trust management, information collection, trust calculation, storage, updating, and distribution, all without the need for a central agent. Conversely, in the centralized approach, a single central entity handles all of these tasks. The semi-distributed approach, on the other hand, relies on a selected group of entities to manage trust, using information received from other network entities.
— **Trust Aggregation Module :** This module handles various versions of trust values for a node propagated through different network paths in the previous phase. The primary models employed include Machine Learning, Game Theory, Hybrid, Statistical, Probabilistic, and Fuzzy Logic models.
— **Trust Update Module :** The Trust Update Module is responsible for real-time adjustments to node trust values, guided by their ongoing behavior and feedback from other nodes. It leverages algorithms like Bayesian networks, decision trees, and neural networks for trust value updates. This module revolves around the management of computed trust scores over time. Essentially, two primary approaches are utilized for updating trust values : Event-driven and Time-driven. In the event-driven approach, all actions (e.g., bidding a service or access, delivering a service, etc.) are treated as events, leading to dynamic trust value updates with the occurrence of each event

in the system. In contrast, the time-driven approach periodically recharges trust values utilizing counter-based strategies without waiting for specific events to trigger the updates.

— **Trust Prediction Module :** This module is dedicated to forecasting trust levels between nodes, relying on specific metrics. Its core function is to estimate whether a trustor will place trust in a given node or not.

— **Trust Evaluation Module :** Typically, the evaluation module draws upon a combination of factors, including direct or local knowledge, global knowledge elements (involving direct and indirect trust), and recommendations obtained by querying the node's neighbors and updating the trust table. Consequently, it computes a recommendation, which is then integrated into the global knowledge. This process contributes to the assessment of an entity's trustworthiness.

— **Trust Formation Module :** The Trust Formation Module is primarily concerned with establishing the trust formula and determining how trust values are to be computed. The trust formula is contingent on selected metrics and attributes, making it adaptable and capable of being either straightforward or complex. This module classifies trust formulas into two primary categories : Single-trust and Multi-trust.

— **Trust Inference Module :** The Trust Inference Module is responsible for deducing the trustworthiness of nodes by considering their trust values along with contextual information. For instance, when a node with a previously high trust value exhibits suspicious behavior, this module may respond by reducing its trust value and categorizing it as untrustworthy.

— **Trust Revocation Module :** The Trust Revocation Module is tasked with withdrawing trust from nodes that have been identified as untrustworthy or malicious. Upon revocation of a node's trust, it is effectively excluded from network participation, and its communication privileges are terminated.

## 2.3 Existing Surveys

This section introduces the most recent comprehensive studies focused on trust management within Internet of Vehicles (IoV) systems. We have condensed the primary discoveries from these research papers into Table 2.3. It is essential to highlight that a relatively small number of articles have given particular attention to trust management endeavors in connected vehicles. These surveys, which explore vehicular networks' security and privacy dimensions, offer valuable insights for our ongoing research. This is especially relevant as we are on the verge of conducting an in-depth analysis of connected vehicles' substantial security challenges in the subsequent section.

### 2.3.1 Contributions of existing surveys

Many surveys have been carried out in the domain of Vehicular networks, as outlined in Table 2.3. The majority of these surveys have explored issues related to security and routing protocols while also providing a comprehensive architectural overview of the Internet of Vehicles (IoV) [31, 32]. Some of these surveys have examined potential security challenges extensively and proposed corresponding solutions [44]. In the authors' work in [34], a comprehensive survey on Vehicular networks has been presented, covering various attack models and offering a qualitative analysis of the security and privacy requirements within identity-based security and privacy schemes. Furthermore, in [36], the authors have provided an all-encompassing survey of existing authentication and privacy schemes, comparing security and privacy criteria, computational overhead, and resilience to various attacks. This chapter also contains a qualitative comparison with previous surveys. Moreover, [40] has delivered comprehensive surveys concentrating on privacy within IoV-based architectures.

### 2.3.2 Comparison with our work

Although there is a wealth of publications addressing trust management in connected vehicles, there needs to be more comprehensive surveys encompassing the diverse facets of trust. In Table 2.4, we conduct a comparative analysis of our research concerning the previously mentioned schemes that focus on trust management in connected vehicles. This comparison is grounded in several critical criteria : trust modules, trust metrics, trust challenges, attacks, open research directions, taxonomy, evaluation criteria, and simulation tools. This evaluation highlights the substantial emphasis placed in our work on the identification, review, classification, and comparison of various trust-based schemes, covering a broad spectrum of trust-related aspects.

TABLE 2.4 – **Comparison of our work with different trust surveys.**

| Comparison aspects | Ref.[37] | Ref.[38] | Ref.[41] | Ref.[42] | Ref.[45] | Ref.[46] | Our survey |
|---|---|---|---|---|---|---|---|
| Modules | | | | | | X | X |
| Metrics | X | X | X | | X | X | X |
| Issues | | | | | X | X | X |
| Attacks | X | X | | X | X | | X |
| Perspectives | | | | X | X | X | X |
| Taxonomy | X | X | X | | X | X | X |
| Analysis parameter | X | | | X | | | X |
| Simulation Tool | X | X | X | | X | | X |

## 2.4 Issues

In this section, we will identify and analyze significant challenges related to security and trust in the context of connected vehicles. We will then present a concise overview of prevalent security attacks and delineate corresponding solutions.

### 2.4.1 Security Issues

In the IoV environment, data is transmitted through a wireless network, which is susceptible to interception by malicious nodes. Consequently, security concerns represent the most paramount challenges within Vehicular networks. Any compromised application in this context can pose grave risks to drivers and passengers. The dynamic and high mobility of vehicles, coupled with a constantly changing network topology, scalability issues, short-duration communication links, and diverse technologies within the network, all contribute to the complexity of detecting malicious attacks. Therefore, safeguarding the security of various entities within vehicular networks, including drivers, passengers, vehicles, roadside units, and traffic management authorities. In the IoV context, exchanged messages must remain unaltered and free from unauthorized insertion or modification by potential attackers. Impersonation attacks, wherein malicious nodes assume the identity of legitimate entities (e.g., posing as emergency responders), and then communicate with other nodes to manipulate their behavior, are a significant concern. Security and privacy in the IoV domain are intricately linked to trust-related issues. Numerous research endeavors have been undertaken in this domain, exploring privacy preservation methods, cryptography-based approaches, pseudonym-based techniques, certificate-less authentication, and identity-based signature methods. These evolving schemes play a pivotal role in ensuring the reliability of connected vehicles, particularly by harnessing the power of emerging technologies and incorporating Artificial Intelligence-enabled techniques.

### 2.4.2 Trust management Issues

In recent years, growing concerns surrounding vehicle privacy and authentication have given rise to the pivotal role of trust models in the Internet of Vehicles (IoV) realm. Despite their increasing importance, these trust models are still in their early developmental stages and encounter several challenges, notably in addressing the security issues they seek to overcome. As a result, the integrity of user interactions in Vehicular networks becomes crucial to establish. Trust models play a key role in overseeing and mitigating the impact of both malicious and selfish nodes, ensuring the dissemination of reliable information throughout the network. Moreover, these models must exhibit robust resistance against various malicious attacks, including but not limited to bad-mouthing, on-off attacks, movement tracking, and message sniffing. For instance, the on-off attack exemplifies a node-behavior attack wherein the objective is to evade a negative reputation by alternating between launching malicious services and exhibiting benign behavior. Similarly, selfish node attacks share the motivation to locate and disrupt communications, resembling the behavior of greedy nodes that obstruct event logging and impede the monitoring of node actions. Another noteworthy attack is the bad-mouthing attack, a reputation-based assault aimed at undermining or diminishing the trust reputation of other nodes within the network by providing unfavorable recommendations about them. Furthermore, a persistent challenge lies in balancing privacy and trust

requirements in connected vehicles. This dilemma arises because private and sensitive user information, such as geographic location and real identity, can potentially be exposed, posing a threat to the trust relationships and communications between nodes.

### 2.4.3 Security attacks in IoV.

Security entails the state of being shielded from potential dangers or threats, encompassing safety measures implemented to ensure protection. In the context of the IoV environment, a complex and heterogeneous system with various vulnerabilities, multiple types of security threats can manifest. Moreover, the unique characteristics of Vehicular networks, including their dynamic nature, scalability, and more, amplify the challenges associated with preventing and detecting these security issues. Numerous researchers have delved into the realm of security attacks in connected vehicles, as documented in the publication titled "Vehicular Network Attacks." Their efforts have aimed to categorize these attacks and propose corresponding solutions. In this subsection, we delineate the security concerns prevalent in Vehicular networks and present a summarized overview of these attacks in Table 5.7.

- **Non-repudiation Attack :** This attack is geared toward denying either the transmission or reception of messages by either the sender or receiver. It has adverse effects on the resources of connected vehicles, particularly by overloading the network bandwidth with multiple retransmissions, leading to delays and performance issues.
- **Spamming Attack :** The nodes in the network send spam messages with the intention of inflating the message transfer rate, causing increased latency, higher bandwidth usage, and leading to multiple collisions within the network.
- **DoS Attack** : DoS is a prevalent attack in the Internet of Vehicles (IoV) wherein either internal or external vehicles deliberately disrupt the network's resources and services, rendering them inaccessible to network users. This is typically achieved by either saturating the communication channel or overwhelming network nodes, making them unavailable for legitimate use.
- **DDoS Attack :** The decentralized and dynamic nature of Vehicular networks presents a significant challenge in dealing with DDoS attacks [147, **?**, **?**, **?**, **?**]. In the Internet of Vehicles (IoV), establishing direct communication among vehicles or using roadside units results in a self-organizing and self-configuring network. While fostering flexibility, this inherent design makes Vehicular networks susceptible to DDoS attacks. In these attacks, numerous malicious nodes flood the network with illegitimate traffic, overpowering legitimate communication channels. This renders it highly challenging, if possible, for vehicles to effectively communicate with each other. DDoS attacks in the context of IoV can manifest in various forms.
- **GPS Spoofing Attack :** In connected vehicles, the integrity of GPS signals is crucial for accurate positioning and location information. The GPS Spoofing attack seeks to undermine the authenticity of GPS signals by overpowering them and manipulating the location data sent by GPS satellites. This attack results in the dissemination of false location information to vehicles, compromising their authentication and potentially leading to misleading navigation and communication within the network.
- **Replay Attack :** In a replay attack, a malicious node intercepts and stores a message received from another node and then repeatedly retransmits the same message. This continuous replaying of messages can make it challenging to correctly identify vehicles, especially in emergency situations. This type of attack has the potential to cause serious incidents, such as collisions, due to the disruption of communication and the misinterpretation of information.
- **Masquerading Attack :** In a masquerading attack, the attacker assumes the identity of a legitimate node, essentially wearing it as a mask to produce false messages that appear authentic. The goal of this attack is to create a black hole in the network, where the malicious actor can deceive other nodes into accepting its deceptive messages as genuine, potentially leading to disruptions and security breaches within the network.
- **Man-in-the-Middle Attack :** In a man-in-the-middle attack, the malicious actor positions themselves between two nodes engaged in V2V communication, allowing them to intercept, modify, or closely inspect the messages being exchanged. This gives the attacker the capability to access and control the entire V2V communication, potentially enabling eavesdropping, data manipulation, and disruption of the communication between the legitimate nodes.
- **Wormhole Attack :** In the context of the Internet of Vehicles (IoV), a wormhole attack is designed to extend the tunneling of packets between two malicious nodes, allowing an attacker to control at least two malicious nodes. In this attack, the malicious nodes incorporate themselves as a part of the reply path, enabling them to manipulate and reroute communication between legitimate nodes. This type of attack can compromise the integrity and security of Vehicular networks by

diverting data through unauthorized pathways controlled by the attacker.

— **Greyhole Attack :** The greyhole attack is a type of attack that involves selectively removing data packets of specific applications, particularly those that are vulnerable to packet loss. Greyhole is categorized as a variant of the Blackhole attack and specifically targets the availability of network resources at the network layer. This attack can disrupt the communication and availability of certain applications or services in the network while allowing other traffic to pass through, making it a strategic and sophisticated form of network-layer manipulation.

— **Jellyfish Attack :** The Jellyfish attack primarily focuses on disrupting the availability of the network layer. There are two main types of Jellyfish attacks.

Packet Reordering Attack : In this type, a malicious node intentionally reorders packets before forwarding them, causing acknowledgments to be received out of sequence. This results in the need for message retransmissions due to the perceived communication disruptions caused by the out-of-sequence acknowledgments.

Periodic Dropping Attack : The periodic dropping attack involves the random discarding of packets during communication processes. Furthermore, it entails the dissemination of inaccurate route congestion information. The deliberate misinformation prompts the Jellyfish node to decide on discarding a portion of packets for a brief duration, consequently extending the timeout period for retransmission. This attack strategy aims to introduce delays and disruptions in communication, potentially resulting in network congestion and performance degradation.

— **Black Hole Attack :** This attack involves the redirection of network traffic by a malicious node. In this attack, the malicious node falsely claims to have the shortest path to a destination and lures data traffic from legitimate users. However, instead of forwarding the data, the malicious node simply declines to contribute to the network, effectively dropping all received packets. This malicious behavior can result in significant disruption to the routing table and negatively impact network availability. The primary target of the black hole attack is the network's availability, as it can lead to the loss of data and a breakdown in communication within the network.

— **Sybil Attack :** The Sybil attack is aimed at injecting false or deceptive information into the network, allowing a malicious node to exert control over the network. This attack directly impacts the information generated and reported by various nodes within the network. As a result, affected vehicular nodes may make incorrect decisions that deviate from the actual scenario, ultimately undermining the efficiency and reliability of the system. The Sybil attack can lead to a distorted and compromised communication environment within the network.

— **Message Tampering Attack :** The message tampering attack is employed when the communication route is congested, and the attacker seeks to clear the road. In this attack, a malicious node modifies or alters a recent message and then sends it to the destination as if it were an authentic message. This attack primarily targets the integrity of messages, causing disruptions in the network, especially because the altered message may be overheard by others in the vicinity. Message tampering can lead to the spread of misleading or harmful information within the network, potentially causing confusion and chaos.

— **Tunneling Attack :** The tunneling attack is designed to compromise the integrity of the system. In this attack, the attacker initiates a private communication and establishes a connection between two segments of the network through an external communication channel referred to as a "tunnel." As a result, nodes that are physically distant from each other can communicate as if they were neighboring nodes. This form of attack significantly disrupts the network's normal operation and may lead to unauthorized or malicious communication channels being established, compromising the network's integrity and security.

— **Greedy Behavior Attack :** In a greedy behavior attack, the attacker exploits the Message Authentication Code (MAC) protocol to gain an unfair advantage by consuming a significant portion of available bandwidth and network resources solely for their benefit. The attacker does this to divert other nodes onto alternate routes, effectively securing a clear communication path for themselves to the destination. This selfish behavior can lead to traffic overloading, collisions on the transmission channel, and delays in the legitimate services of registered users, significantly degrading network performance and fairness.

— **Illusion Attack :** The illusion attack involves receiving legitimate data from antennas and simultaneously collecting malicious data from sensors. The attacker then generates false traffic warning messages by utilizing the existing road infrastructure. These deceptive messages can create an illusion for the vehicles on the road. Since drivers' behaviors often depend on the accuracy of the traffic warning messages they receive, this attack can result in vehicle accidents, traffic congestion,

and a reduction in the overall system's performance. The goal of the illusion attack is to disrupt the normal flow of traffic and compromise the safety and efficiency of the vehicular communication system.

— **Traffic Analysis Attack :** In a traffic analysis attack, the attacker actively listens to message transmissions and analyzes the frequency and patterns of communication to extract maximum useful information. This type of attack is particularly dangerous as it poses a significant threat to the confidentiality and privacy of communications within Vehicular networks. By monitoring and analyzing network traffic, the attacker can gain insights into sensitive information and potentially compromise the privacy and security of network users.

— **Jamming Attack :** The jamming attack is designed to disrupt the communication channel in Vehicular networks by sending a highly powered signal on the same frequency, effectively lowering the signal-to-noise ratio for the intended receiver. This attack aims to interfere with regular communication by overwhelming the signal with noise. This attack is particularly dangerous because it does not adhere to the rules of valid safety alerts, making it a severe threat to safety-critical applications within the Vehicular network. Jamming attacks can have serious consequences for safety-related communications and applications.

— **Impersonation Attack :** In an impersonation attack, some vehicles pretend to be emergency entities or other trusted entities to attract other vehicles into communicating with them and potentially influence their behavior. This type of attack relies on techniques like Building up a Secure Connection along with Key Factors (BUCK) Filter. The BUCK Filter detects impersonation attacks by broadcasting beacons and accurately determining the position of the messaged vehicle. Once a fraudulent node is detected, it is isolated from the communication environment to prevent further deceptive behavior and protect the integrity of the network.

— **Free Riding Attack :** A free riding attack takes place through fraudulent authentication attempts when connected to cooperative message authentication. In this attack, the malicious entity exploits the authentication efforts of other legitimate users without making their own contributions. This type of attack is a significant threat to cooperative message authentication, as it undermines the fairness and effectiveness of the authentication process and may allow malicious actors to gain unauthorized access to network resources.

— **Replication Attack :** In a replication attack, a malicious node's objective is to introduce additional nodes into the network illegitimately. To achieve this, the attacker utilizes the identity of another node that is already present legally in the network to transmit false messages to the network. The attacker may use duplicate keys and/or certificates of other legitimate users to create uncertainty in the system. This not only makes it difficult for traffic authorities to identify the vehicle but also causes confusion for the Trusted Authority (TA), which is responsible for maintaining trust and security within the network. Replication attacks can lead to various security and communication issues within the network.

— **Eavesdropping Attack :** Eavesdropping is a common and serious attack in Vehicular networks, primarily targeting confidentiality. The goal of this attack is to intercept and obtain confidential information from the protected data of vehicles. Non-registered or unauthorized users may exploit this attack to access sensitive details, such as user identities and data locations. This information can then be used for tracking vehicles and executing various attacks, posing a significant risk to the privacy and security of network users. Eavesdropping attacks undermine the confidentiality and integrity of communications within Vehicular networks.

## 2.5 Classification

Presently, three primary trust management approaches are in active use : Entity-based schemes, Data-based schemes, and Hybrid schemes. In this section, we will provide an overview of these categories and explore a proposed taxonomy that relies on technology utilization, specifically focusing on emerging technologies and Artificial Intelligence.

### 2.5.1 Entity-based schemes

Entity-based trust management approaches focus on establishing trust at the level of individual nodes within a network. In these approaches, each entity or node maintains its trust value, which evolves over time. Trust levels for these nodes are determined using reputation-based trust metrics, with trust and reputation often being critical factors in assessing their trustworthiness. This trust calculation relies on various historical metrics, including the node's past behavior and activities and the recommendations

TABLE 2.5 – **Threats and attacks regarding security in Vehicular networks.**

| Layer | Attack name | Attacks on | C. service | Solution |
|---|---|---|---|---|
| Physical | Jamming | Sensors input in vehicle | Authentication | [49] |
| | Impersonation | Infrastructure | Authentication | [50] |
| | Free riding | Infrastructure | Authentication | [51] |
| | Replication | Infrastructure | Availability | [52] |
| | Eavesdropping | Wireless interface | Confidentiality | [53] |
| | Man in the middle | Infrastructure | Confidentiality | [54] |
| Data Link | Traffics analysis | Infrastructure | Availability | [55] |
| | Illusion | Sensors input in vehicle | Confidentiality | [56] |
| | Greedy behaviour | Wireless interface, hardware and software | Authentication | [57] |
| Networking | Tunneling | Wireless interface | Authentication | [58] |
| | Sybil | Wireless interface | Authentication | [59] |
| | Message Tampering | Infrastructure | Authentication | [60] |
| | Black hole | Wireless interface, hardware and software | Availability | [61] |
| | Jellyfish | Infrastructure | Availability | [62] |
| | Grey hole | Wireless interface, hardware and software | Availability | [63] |
| | Wormhole | Hardware and software | Availability | [64] |
| Transport | Masquerading | Infrastructure | Confidentiality | [65] |
| | Replay | Hardware and software | Data integrity | [66] |
| | GPS Spoofing | Sensors input in vehicle | Data integrity | [67] |
| | DoS | Wireless interface | Authentication | [68] |
| | DDoS | Wireless interface | Availability | [69] |
| | Spamming | Wireless interface | Availability | [70] |
| Application | Non-repudiation | Infrastructure | Repudiation | [71] |

exchanged among different entities. For instance, in a cluster of vehicles, a vehicle may trust all other vehicles within the identical cluster better than those in diverse clusters.

In the work presented in [72], the authors introduce a trust inference scheme designed to withstand attacks in Vehicular Networks. This approach is based on subjective trust derived from historical interactions and recommendation trust obtained from the opinions of neighboring nodes. Additionally, the authors propose a trust-aware multicast routing protocol.

In [73], the authors introduce a similarity-based scheme to mitigate the injection of false information and assess the trustworthiness of safety-event reports in the network. The trust model generates a similarity rating based on periodic beacons containing location and speed information and uses the echo protocol to validate the reports produced.

In [74], the authors propose a trust model based on a trusted authority node responsible for managing reputation scores. This authority determines whether a particular participant node is granted access to the network or revoked. A low reputation score signifies an untrusted node to be excluded, while a high or acceptable reputation score signifies credibility for network access and communication.

In [75], the authors integrate the concept of highway platooning. Platoon head vehicles are ranked based on reputation metrics, and the trust model introduces a special server for assessing the trustworthiness of platoon head vehicles. Reputation calculations rely on gathering feedback from vehicle users, with an iterative filter in place to exclude feedback from malicious nodes. Consequently, a reliable platoon head vehicle is recommended by the server node.

On the other hand, data-based trust management schemes focus on evaluating the trustworthiness of the data generated by an entity rather than the entity itself. In these schemes, trust is closely linked to the content of the messages produced, making data authenticity a critical requirement. Data-based trust models assess the trustworthiness of data content based on its utility, which is determined by factors such as time, proximity, the type of event, and the role of the node. Data trust evaluation is particularly convenient in Vehicular networks, as strong social connections are often lacking among rapidly moving entities.

In [76], a data-based scheme is presented. This model detects malicious nodes in Vehicular networks by comparing the similarity of messages. It assesses the similarity between messages received from nearby vehicles and self-reported messages. Nodes calculate their flow values based on speed and density parameters and compare these values with received messages, reporting mismatched messages to the sender.

In [77], the trust model is constructed based on location, proximity, location verification, and time closeness. Receivers assess their confidence in each reported event by a particular sender, assigning distinctive trust values to each message related to a reported event. The technique then ranks the calculated trust weights to make judgments in favor of the respective messages.

Authors in [78] present an intrusion-aware strategy to ensure trust requirements in Vehicular networks. The trust assessment relies on the confidence and trust values assigned to each piece of content about a specific event. Parameters like location proximity, data freshness, location correctness, and time verification are considered in the trust formula. Based on the sender node number and their confidence values, the trust value is calculated, and the receiver decides whether to accept or block the message.

In [79], the authors introduce a trust model based on the Tanimoto coefficient, where trust values are disseminated, built, and used by Roadside Units (RSUs) and vehicles working in cooperation within the network. These trust values are determined after inspecting reported events and beacons.

### 2.5.2 Hybrid schemes

These types aim to combine the assessment of trustworthiness at both the entity and data levels. These schemes seek to provide an efficient method for evaluating trust that takes into account not only the content of the messages but also the trustworthiness of the entities involved. This is particularly valuable in networks like Vehicular networks, where data that has been evaluated as trustworthy by multiple trusted entities is shared as reliable with other network nodes.

In [80], the authors introduce a hybrid scheme with a focus on enhancing trust management efficiency in Vehicular networks, particularly in the decision-making process. This scheme requires decisions to be made within specific time slots or when multiple messages exceed predefined thresholds.

In [81], researchers present a scheme that incorporates both the trustworthiness of vehicles and the trustworthiness of data. This approach involves a behavior assessment process and the calculation of a similarity rating. Trust evaluation is based on data analysis using the Dempster-Shafer Theory (DST). Data trustworthiness is assessed through the similarity of reported traffic information, while node trustworthiness is expressed using functional trust, indicating the likelihood that a vehicle will exhibit appropriate behavior. This is determined by assessing observed misbehaviors by neighboring nodes and applying combined filtering-based recommendation trust. Cosine similarity is a critical factor in evaluating the

credibility of recommendations, especially in trust rate calculation and trusted neighbor selection. Predicted trust rate computations are used to define the recommendation trust.

In [82], authors combine behavior and similarity factors to present a robust hybrid trust management scheme for Vehicular networks. This scheme is designed to detect malicious data injected through Sybil attacks. Trust values are assigned by verifying the similarity between the expected and actual behavior of a vehicle, such as the driver's responses to traffic signals, and the similarity of messages generated by neighboring vehicles.

In [83], researchers introduce a model that focuses on ensuring location privacy in Vehicular networks. It calculates entity trust values by assessing and verifying the probability of event and beacon messages. Trust assessment of the sender's entity beacon messages is based on the Cosine similarity technique. Trust calculations take into account position, velocity, drive direction values, and recorded trust information from neighboring vehicles' beacons. Data trust is evaluated in two dimensions : direct trust, which is based on event and beacons directly received, and recommendation trust, which is estimated based on vehicle recommendations. The Dempster-Shafer Theory (DST) is applied to merge direct and indirect trust values to obtain the final trust score and initiate the decision phase based on a trust threshold value.

### 2.5.3 Technology-based classification

Artificial Intelligence and cutting-edge technologies, including Cloud Computing, SDN, Fog/Edge Computing, and Blockchain, are recognized as valuable assets for crafting resilient trust frameworks. In this section, we examine recent methodologies employed in each of these technologies.

#### 2.5.3.1 Cloud-based schemes

In [84], the authors utilize cloud technology to establish a trust framework based on the interconnections among autonomous, interconnected vehicles. This framework is structured into three key layers : the cloud layer, the communication layer, and the physical layer. The authors introduce the "fliplt" game to capture interactions among the services in the cloud layer, with a focus on enhancing security in the face of potential threats. Within the communication layer, they elucidate the diverse communication channels between cloud servers and connected vehicles. In this layer, the authors introduce a trust model that relies on reputation and knowledge, employing a signaling game to evaluate the reliability of cloud services. The physical layer oversees the performance of the participating devices, including attackers and defenders in the signaling game. Decision-making primarily hinges on the performance of both the cloud and physical layers.

In [85], the authors present a trust management approach tailored for Vehicular Networks, with a specific emphasis on the computation process. This solution encompasses three sequential steps. The initial phase involves data preprocessing using the Dempster-Shafer Theory (DST). In the subsequent stage, the authors employ a Fuzzy analyzer to compute trust values for nodes within the network, incorporating both direct and indirect trust assessments. In the third phase, they implement reward and penalty algorithms to incentivize honest vehicles while penalizing malicious ones. Notably, this approach allows any vehicle to request the trust value of a neighboring node through cloud servers.

Another cloud-centric trust management strategy is introduced in [86]. This work is structured around three layers and two trust managers : a central cloud layer, a roadside cloud layer, a vehicle cloud layer, and global and domain trust managers. The first layer encompasses the communication history and trust lists of all vehicles, overseen by the global trust manager. The domain trust manager and the roadside cloud layer manage various trust value requests, including those related to neighboring, friends, and historical trust. The roadside cloud layer is responsible for creating vehicular virtual machines. The overall trust level is determined at the vehicle cloud layer, where a vehicle can solicit the trustworthiness of the message sender from a vehicular virtual machine. This machine computes trust values for neighboring and friend nodes and accesses historical trust values from a central server. Subsequently, it furnishes the requester vehicle with the comprehensive trust value of the requested node, updating it as needed.

In [87], the authors harness cloud technology to introduce an agent-based intelligent approach to trust management. This approach involves two principal agents : mobile and static agents, which evaluate the trustworthiness of both the cloud service provider and the user. They rely on direct trust, which is based on the past account transactions, and indirect trust, calculated by the mobile agent, to determine the cumulative trust value.

TABLE 2.6 – **Basic trust managements schemes in Vehicular networks.**

| Ref. | Class | Used metrics | Tools | Simulator | E. parameters |
|---|---|---|---|---|---|
| [72] | Entity | Reputation, knowledge | Markov process | SUMO, NS-2 : | Detection rate |
| [73] | | Node proprieties | Association rule mining and echo protocol | SUMO | Success rate |
| [74] | | Reputation | Elliptic curve method | Not specified | Computation and communication cost |
| [75] | | Reputation | Iterative filtering method | MATLAB | QoS of vehicles, accuracy level and resistance to bad-mouthing and ballot stuffing attack |
| [76] | Data | Node properties, proximity, environment-factors. | Defined formulas and signature-based | OMNET++, SUMO, VACaMobi | Average density and success rate. |
| [77] | | Proximity | Defined formulas and signature-based | SWAN++ | false location detection accuracy, false positive rate |
| [78] | | Location | Defined formulas | Not provided | Time complexity and false node impact on trust. |
| [79] | | Beacon | Tanimoto coefficient | NS-2, SUMO | Precision, recall, Detection delay |
| [80] | Hybrid | Reputation, event | Decision making process | NS-2 | Detection accuracy, decision delay |
| [81] | | Reputation, knowledge, environment | DST-based, osine similarity rule | GloMoSim | Precision, recall, communication overhead |
| [82] | | knowledge+node proprieties | Defined formulas, stochastic cellular | Automata Model | detection rate,average delay |
| [83] | | Beacon+event+reputation | Cosine similarity rule,signature-based | NS-2 | attacks detection rate, misbehaving vehicle rate, detection delay |

#### 2.5.3.2 SDN-based schemes

In their study documented in [88], the researchers harnessed the power of SDN (Software-Defined Networking) technology and employed deep reinforcement learning techniques to develop a holistic solution aimed at addressing trust establishment and path learning in Vehicular networks. Through the integration of SDN, they successfully separated the data and control planes, providing a more adaptable and centralized approach to managing network operations. In this configuration, a centralized controller incorporates a deep reinforcement learning algorithm, enabling all legitimate vehicles in the network to determine the most trustworthy path for data transfer. This, in turn, enhances the efficiency of data exchange among the vehicles.

To assess trust values, the authors applied a Q-learning-based convolutional neural network algorithm, a form of reinforcement learning. These trust values were derived from the ratios of forwarded packets, aiding in the evaluation of network path reliability and trustworthiness. Essentially, their approach leveraged the capabilities of SDN and deep reinforcement learning to optimize trust management and path selection in Vehicular networks, ultimately contributing to the network's efficiency and reliability.

In [90], the researchers utilized SDN (Software-Defined Networking) to improve network performance by incorporating an on-demand distance vector routing method. Their approach encompasses three fundamental layers : data, control, and application. The data layer handles data forwarding, the control layer manages data routing and network topology, and the application layer oversees routing protocol control. Trust values are computed based on ratios pertaining to both data and control packet forwarding, enabling the assessment of network path reliability and trustworthiness. This, in turn, enhances network performance and security.

In their work described in [91], the authors introduced an SDN-based scheme that combines a geographic routing protocol with SDN capabilities to establish a routing process centered on a trust management model and encryption functions. Their approach also incorporates a clustering concept, where network nodes are organized into distinct clusters, each comprising an elected cluster head and cluster nodes. The cluster head serves as a semi-centralized controller responsible for managing communication and maintaining an error log of network operations. The selection of the cluster head is determined by a map factor, which evaluates various factors, including a vehicle's possession of its public key and the weights of its neighboring nodes. These weight values are computed based on the load capacity determined by trust levels and the reception of beacons. Moreover, past interactions recorded in the error log play a crucial role in evaluating trustworthiness within the network, enhancing the reliability and security of network operations. This amalgamation of geographic routing, SDN, and trust management augments the efficiency and trustworthiness of communication within Vehicular networks.

#### 2.5.3.3 Fog/Edge-based schemes

In [92], the researchers made use of Edge/Fog technology to enhance trust management within Vehicular Networks. Their approach centers on executing reputation management through local servers. Edge servers are organized by trusted local authorities to facilitate the trust establishment process. Each node uploads segments of its reputation to the nearest local authority, which aggregates, updates, and stores them in a global reputation dataset concurrently. This allows each vehicle to access the most up-to-date reputation value of another passing node before engaging in any collaborative activities.

In [93], the authors employed a bidding price-based method to bolster trust in Fog services. This work integrates the necessity for certificates by vehicles to ensure the registration of legitimate nodes for conducting Fog services transactions. Once registered with digital currency, accepted vehicles gain the privilege to engage in activities within the uncovered zone. The utilization of infrastructure-based Fog node resources is imperative to enhance the utilization of Fog services. Trust calculation in the rural zone is contingent on metrics such as transaction records, node types, and bidding numbers, alongside the consideration of global transactions (e.g., infrastructure-based Fog nodes). Any malicious activities within the network may expose the actors' bidding, resulting in trust erosion and compensation for the affected parties.

In [94], the authors harnessed Fog computing technology to manage trust in Vehicular networks. This system comprises two layers : one encompassing the communication system, which includes a Cloud server and trusted authorities, and the other formed by vehicles and Edge nodes. Trust values for both the sender and the message are computed using predefined Fuzzy rules that take into account parameters such as location verification, vehicle type, and experience. Each registered vehicle is assigned an authentication level by the Edge nodes, which can be queried by the receiving vehicle to make informed decisions. The authors incorporated the Cuckoo filter to enhance system performance against the generated data volume and applied the k-nearest neighbors algorithm to mitigate line-of-sight issues.

In [95], the authors harnessed the capabilities of Fog Computing and the proximity of edge users to select the most capable node. This approach reduces the burden on vehicles, such as trust assessment for the sender and the dissemination of event details. Trust evaluations conducted by local vehicles are gathered by the fog node, enabling vehicles to carry out specific tasks locally and diminishing the necessity for frequent communication with the cloud. The trust scheme is anchored in the reputation of vehicles' performance, utilizing the Task-based Experience Reputation (TER) method. The implementation of TER in this work reduces message transmission overhead and alleviates the workload on the vehicles.

#### 2.5.3.4 Blockchain-based schemes

The incorporation of Blockchain technology for trust management in Vehicular Networks is capturing the growing interest of researchers. Below, we highlight some noteworthy examples of Blockchain's utilization in enhancing trust management within Vehicular Networks :

In [96], the authors harnessed Blockchain technology to boost privacy in Vehicular Networks by establishing a reputation management system. This system revolves around two primary entities : the certificate authority, responsible for certificate generation and management, and the law enforcement authority, overseeing vehicle registration and reputation assessment. The law authority maintains a dataset containing information pertaining to real identities, public keys of registered nodes, certificate issuance and revocation, as well as message exchanges. A reputation management framework, guided by an anonymous authentication algorithm, incentivizes trust-building through reward and punishment mechanisms.

In [97], a regional federated learning approach is employed to bolster security and preserve privacy in the network. Vehicle training models are distributed across various regions, and their trustworthiness is upheld through a robust mechanism.

In [98], the authors combined Blockchain and deep learning technologies to fortify trust management in Vehicular Networks. Nodes possess the capability to report malicious nodes to the RSU entity after scrutinizing messages received from nearby vehicles. Blockchain technology is used to verify the authenticity of these reports, ensuring accurate revocation of malicious nodes within the network by the RSU.

In [99], a resilient system is introduced with several key steps, including generating and uploading ratings, computing trust value offsets, electing miners, generating new blocks, and implementing a consensus algorithm. Bayesian inference is employed to gauge the credibility of received messages, assigning specific ratings to each message before uploading them to the RSU. Trust value offsets are computed using weighted aggregation and are encapsulated into a single block. The miner election process determines the node responsible for generating a new offset block, with the RSU typically having a greater stake due to the consensus mechanism's consideration of offset absolute values as stakes. This new offset block is then appended to the trust Blockchain, and the consensus algorithm is applied to enhance resistance against simultaneous block reception.

These methodologies underscore the growing significance of Blockchain technology in enhancing trust management within Vehicular Networks, offering solutions that bolster network security, privacy, and trustworthiness.

#### 2.5.3.5 Artificial Intelligence-based schemes

In the realm of trust management within Vehicular Networks, AI-based methodologies seamlessly merge various techniques such as clustering and reinforcement learning, fuzzy logic, and game theory to enhance overall performance.

**Clustering and Reinforcement Learning-based schemes** In [100], the authors harnessed stability and clustering algorithms to effectively manage trust in Vehicular Networks, with a specific focus on metrics related to communication and data trust. Their trust model comprises three essential phases : neighborhood discovery, cluster head election, and stability maintenance. During the neighborhood discovery phase, the model exclusively considers neighboring vehicles traveling in the same direction. In the cluster head election phase, a trust score is calculated using a backoff timer, factoring in variables like reputation, direction similarity, and mobility. To ensure cluster stability, the authors implemented two key components : a Beta reputation system that oversees cooperative behaviors among vehicles and an event reputation-based system with severity metrics to assess the reliability of exchanged information.

In a similar clustering-based approach presented in [101], the authors introduced a composite metric to determine trustworthiness values for individual vehicles and associated resources. In this framework, neighboring vehicles assign trust scores to each node based on behavior-based metrics, resulting in precise trust scores for all participating nodes. The approach also considers computational resources, taking into

account factors like node link capacity and remaining power to predict future resource requirements. Cluster head election in this method is determined by the composite value, with the node possessing the highest composite value being designated as the cluster head.

Moving to [102], the authors introduced a collaborative intrusion detection system for Vehicular Networks that leverages ensemble learning and shared knowledge techniques. Participating nodes aggregate rating scores using a voting scheme to create a set of weighted random forest classifiers. Each vehicle trains its local classifiers and communicates its knowledge as a trust factor, enabling the system to collectively detect and respond to intrusions.

In [103], a scheme was introduced that integrates crewless aerial vehicles to aid in routing and identifying dishonest vehicles, particularly in scenarios involving road disconnections. This scheme encompasses two primary routing modes : data routing among vehicles with the assistance of crewless aerial vehicles to reduce delay and overhead, and data routing among crewless aerial vehicles themselves. The selection of cluster heads by crewless aerial vehicles is based on speed, position, and trust parameters. The authors applied the ant colony optimization algorithm to enhance the routing process, and trust scores rely on knowledge and recommendations, leading to more efficient and reliable communication within Vehicular Networks.

**Fuzzy Logic-based schemes** In [104], the authors presented a trust management approach that utilizes fuzzy logic techniques to assess the credibility of exchanged data in Vehicular Networks. In this method, each node encrypts its transmitted data with a unique identifier, which the receiving node then verifies. Trust evaluation incorporates various behavioral metrics, including cooperativeness, honesty, and responsibility. A node with a high trust value is considered an excellent cooperative node. Honesty is gauged by the percentage of transmitted honest packets, and a responsible node is defined as one with a high percentage of detected event reports. The fuzzy logic process in this solution entails calculating these metrics and converting them into fuzzy values, which are subsequently used to apply fuzzy rules. The final trust value is determined after the defuzzification phase.

Another fuzzy logic-based approach was introduced in [105]. In this scheme, the authors model malicious behaviors of nodes using three trust factors represented by fuzzy sets. Trust calculation relies on a fuzzy-logic algorithm, with particular emphasis on the impact of content modification. The effect of content modification is quantified by a specific parameter to assess its influence on trust estimation. This approach demonstrated impressive precision, recall, and accuracy rates in trust management.

In [106], the authors proposed a robust authentication scheme using fuzzy logic to safeguard users from malicious nodes in Vehicular Networks. They developed a fuzzy-based authentication algorithm for detecting malicious nodes based on the Mamdani Fuzzy Inference technique. The authors conducted simulations using MATLAB to validate the effectiveness of this technique. This approach permits only honest nodes to transmit data and engage with other nodes within the network.

In [107], the authors introduced a trust protocol called Fuzzy Trust Optimized Link State Routing (FT-OLSR), which extends the OLSR security protocol. In this approach, each node calculates the trust score of its one-hop neighboring nodes by exchanging control messages using the FT-OLSR routing protocol. Simulations conducted in NS-2 demonstrated that incorporating fuzzy logic into the OLSR routing protocol enhanced its performance in trust management and routing within Vehicular Networks.

**Game Theory-based schemes** In [108], the authors introduced a theory-based game approach to enhance communication security in the Internet of Vehicles (IoV), leveraging the hedonic coalition model. This solution involves forming collaborative coalitions of vehicles by integrating trust among them to improve trust relationships and encourage participation in coalitions within the system. Trust values are evaluated using a Bayesian inference filter, considering direct historical interactions. The receiver vehicle assesses the transmitted message's content against the real event state and updates the sender vehicle's trustworthiness score using the incomplete beta function. The authors also introduced a mechanism for penalizing newly joining nodes with no historical interactions. Trust score changes are captured, and new coalitions are formed by periodically executing the coalition algorithm. The final coalition composition is based on vehicle trustworthiness and their preference relations, with shifting rules enabling vehicles to switch between coalitions.

In [109], a multi-layered intrusion detection scheme for Vehicular Networks is introduced. Game theory techniques are applied alongside a distributed Cluster Head (CH) selection algorithm to identify malicious nodes using a lightweight neural network classifier. The Vickey-Clarke-Groves method is employed to enhance the performance of vehicle cluster head selection. Reputation values held by Roadside Units (RSUs) are used to assess the trustworthiness of the CHs.

In [110], the authors presented a theory-based game scheme for trust management in the IoV system, utilizing an evolutionary game framework within a reputation-based trust model. This model simulates the dynamic protection system and provides models for attacking strategies by malicious nodes. It assigns trust scores to vehicles and traffic-related event messages, and introduces a punitive algorithm for vehicles sending false reports or deleting sent messages, resulting in decreased trust scores. The scheme takes into account the deception intensity, representing a vehicle's capability to deceive other nodes and falsify event reports. The system evolves to enhance the joining or rejoining process and to eliminate dishonest nodes.

In [111], the authors introduced a trust management scheme to enhance the performance of vehicles in estimating trust values of other nodes using a reputation-based method and assessing legitimate messages. Certainty plays a crucial role in trust evaluation, incorporating both direct and indirect reputation sources. Direct reputation information is derived from direct interactions and stored in historical communication tables, while indirect reputation is based on neighbor ratings and RSU recommendations. A Fuzzy C-means clustering technique is used to identify trustworthy reported messages in the indirect-reputation establishment. Computed scores are combined using uncertain deductive theory. The legitimacy of received messages is evaluated using the K-means algorithm, forwarding only those with a reputation level exceeding a predefined threshold. The authors also introduced an incentive scheme based on evolutionary game theory, combining nodes clustering, adopted methods, and payoff calculation modules to encourage nodes' cooperation.

## 2.6 Discussion

The comprehensive survey presented earlier underscores the critical role of trust management in upholding network reliability. Within this survey, we have summarized, compared, and deliberated upon the various trust management schemes detailed in Table 2.6, Table 2.7, Table 2.8, Table 2.9, and Table 2.10. As the integration of multiple technologies becomes more prevalent within network infrastructure, it simultaneously introduces novel security and privacy challenges that must be addressed proactively.

### 2.6.1 Summary

We have compiled a summary of the surveyed schemes, categorizing them based on specific criteria, which include the approach's category (basic or emerging/AI-based approach), class of the approach (entity-based, data-based, or hybrid), the trust metrics utilized, the tools employed, simulator used, and the evaluation parameters (E. parameters). This comprehensive summary is presented in Table 2.6, Table 2.7, and Table 2.8. The purpose of this summary is to facilitate a qualitative comparison between these approaches in the subsequent subsection.

### 2.6.2 Comparison

This subsection is designed to present a qualitative comparison among the summarized approaches, focusing on key factors such as scalability, dynamicity, privacy, complexity, computation overhead, and robustness, as outlined in Table 2.9 and Table 2.10. By examining these critical aspects, we aim to provide insights into how these approaches measure up against one another in terms of their performance and suitability for various network scenarios.

In this subsection, we will engage in a comprehensive discussion of the surveyed trust management approaches, using a specific set of criteria for evaluation. These criteria include privacy, scalability, dynamicity, complexity, communication overhead, and efficiency. By delving into these factors, we aim to provide a thorough assessment of each approach's strengths and weaknesses, helping to guide the understanding of their suitability for various network scenarios.

Privacy remains a paramount concern in the context of future connected vehicle networks, and as such, privacy preservation is a critical requirement for trust management schemes. An analysis of the approaches outlined in Table 2.9 and Table 2.10 reveals that a significant portion (30%) of the surveyed papers lack robust privacy protection measures. However, certain works, such as those cited in [74, 77, 78, 79, 83, 92, 94, 95, 96, 105, 107, 108, 109], exhibit substantial efforts in safeguarding users' credentials and privacy.

Dynamicity is another key criterion, and it's noteworthy that most of the surveyed schemes meet dynamicity requirements. These approaches demonstrate flexibility through features like lower infrastructure support, dynamic trust metrics, and swift trust value updates. Data-based models, in particular, tend to excel in dynamicity compared to entity-based models, as they require fewer exchanges between nodes

TABLE 2.7 – **Emerging technology-based trust management schemes in Vehicular networks.**

| Ref. | Class | Used metrics | Tools | Simulator | E. parameters |
|---|---|---|---|---|---|
| [84] | Cloud | Reputation, knowledge | Flipit and signaling game | MATLAB | Cloud's controlling service probability |
| [85] | | Reputation,knowledge and event | DST-based and fuzzy rules | Java-based | Response time,trust value change |
| [86] | | Reputation,knowledge | Defined formulas | Performance Evaluation,Process Algebra | Throughput and response time |
| [87] | | Node proprieties | DST-based | Not available | Not available |
| [88] | SDN | Knowledge and node properties | Q-learning | TensorFlow, OPNET | Throughput |
| [89] | | Knowledge and node properties | Deep Q-learning and Markov decision process | TensorFlow | Convergence performance and delay |
| [90] | | Node proprieties | Defined formulas | OPNET | Throughput, total messages sent |
| [91] | | Knowledge | Clustering scheme and signature based | NS-2.34 and Vehicular Network MobiSim | Packet delivery ratio and average end to end delay |
| [92] | Fog/Edge Computing | Node proprieties | Signature-based bidding price | Not available | Transactions, attacks number |
| [93] | | Reputation | Multi-weighted subjective logic | Not available | Average reputation value adn Detection rate |
| [94] | | Knowledge node proprieties and event | Fuzzy logic and K-nearest neighbour algorithm | NS-2 SUMO MOVE | Precision Recall overhead |
| [95] | | Node properties and reputation | Task-based Experience Reputation (TER) | NS-2 | Overhead and workload of messages. |
| [96] | Blockchain | Reputation and knowledge | Proof-of-work signature-based SHA-256 | Not available | Storage and transmission overhead |
| [97] | | Reputation | Regional FL algorithm signature-based | Not available | Model accuracy rate |
| [98] | | Node proprieties | Deep Learning (FeedForward Neural Network | NS-2, SUMO | Precision, Recall of malicious nodes detection |
| [99] | | Node proprieties | Proof of Work and Proof of stake,SHA-256,Bayesian inference | Matlab-based | unfair ratings vs false reports rates |

TABLE 2.8 – **AI-based trust management schemes in Vehicular networks.**

| Ref. | Class | Used metrics | Tools | Simulator | E. parameters |
|---|---|---|---|---|---|
| [100] | Clustering | Reputation, node proprieties | Defined formulas | Omnet++ | CH's election time and duration, rate of malicious nodes elected as CH, delivery rate. |
| [101] | | Knowledge, node proprieties | Defined formulas | Matlab-based | Trust metric value with dishonest vehicles. |
| [102] | | knowledge | Learning ensemble | SUMO | Dishonest nodes detection rate, False Negatives, False positives, dishonest vehicles detection accuracy. |
| [103] | | Reputation, Knowledge | Optimization colony | NS-2, MobiSim | Communication overhead, dishonest nodes detection rate, hops' number average, packet delivery rate, end to end delay. |
| [104] | Fuzzy Logic | Knowledge, Reputation | Defined formulas | NS-2, SUMO, MOVE | Behaviour of correlation, detection accuracy with and without collusion. |
| [105] | | Knowledge, node proprieties | Fuzzy logic-based algorithm | NS-2, SUMO | Dishonest nodes detection rate, precision, Recall, accuracy. |
| [106] | | Reputation, node proprieties | Mamdani Fuzzy Inference | MATLAB | Malicious nodes detection rate, accuracy |
| [107] | | Reputation | Fuzzy logic,FT-OLSR | NS-2 | Delay, packet delivery rate |
| [108] | Game theory | Knowledge | Bayesian inference filter | Matlab | Computation's time, compromised decision's rate |
| [109] | | Reputation | Vickrey–Clarke–Groves, Neural Network | NS-3, SUMO | True positives, true negatives, false alarm rate,malicious nodes' detection rate. |
| [110] | | Reputation | Defined formulas | Evolutionary game-theory model | Overall utility's growth rate, nodes' strategy change. |
| [111] | | Reputation | K-means algorithm, fuzzy C-means clustering, defined factors | MobiSim, NS-2 | Decision making's accuracy rate, throughput, false alarm's rate, forwarding rate, packet delivery delay. |

TABLE 2.9 – **Comparison of different surveyed trust management schemes in Vehicular networks.**

| Ref. | Year | Category | Privacy | Dynamic | Scalable | Complex | Overhead | Efficient |
|---|---|---|---|---|---|---|---|---|
| [72] | 2019 | Entity-based | | X | | X | X | X |
| [73] | 2015 | | | X | X | | | |
| [74] | 2019 | | X | X | | X | X | X |
| [75] | 2016 | | | X | | | | X |
| [76] | 2014 | Data-based | | X | X | | | |
| [77] | 2014 | | X | X | | X | | X |
| [78] | 2012 | | X | X | X | X | X | |
| [79] | 2013 | | X | X | | X | | X |
| [80] | 2014 | Hybrid | | X | | X | | X |
| [81] | 2015 | | | X | X | X | X | X |
| [82] | 2016 | | | X | X | | | X |
| [83] | 2013 | | X | X | X | | | |
| [84] | 2019 | Cloud | | X | | | | |
| [85] | 2019 | | | X | X | X | | X |
| [86] | 2017 | | | X | | X | | X |
| [87] | 2017 | | | X | | | | |
| [88] | 2018 | SDN | | X | | | X | X |
| [89] | 2022 | | | X | | X | X | X |
| [90] | 2016 | | | X | | X | | |
| [91] | 2020 | | | X | | X | X | X |
| [92] | 2017 | Fog/Edge | X | X | | X | X | X |
| [93] | 2019 | | | X | X | | X | X |
| [94] | 2020 | | X | X | X | X | X | X |
| [95] | 2021 | | X | X | X | | X | X |

TABLE 2.10 – **Continued Table.9**

| Ref. | Year | Category | Privacy | Dynamic | Scalable | Complex | Overhead | Efficient |
|---|---|---|---|---|---|---|---|---|
| [96] | 2018 | Blockchain | X | X | | | X | X |
| [97] | 2021 | | | X | | | | X |
| [98] | 2020 | | | X | X | | | X |
| [99] | 2018 | | | X | X | X | X | X |
| [100] | 2018 | Clustering | | X | X | | | X |
| [101] | 2019 | | | X | X | X | X | X |
| [102] | 2020 | | | X | | | X | X |
| [103] | 2021 | | | X | | X | X | X |
| [104] | 2017 | Fuzzy-Logic | | X | X | | | X |
| [105] | 2021 | | X | X | X | | X | X |
| [106] | 2022 | | | X | X | X | X | X |
| [107] | 2019 | | X | X | X | X | X | X |
| [108] | 2019 | Game theory | X | X | X | | X | X |
| [109] | 2018 | | X | X | X | | | X |
| [110] | 2019 | | | X | | | | X |
| [111] | 2019 | | | X | | | X | X |

to derive global trust. Nevertheless, reputation-based models might face challenges in maintaining trust assessments for highly mobile nodes, which can result in connection losses.

Scalability, which gauges the network's ability to accommodate an increasing number of communicating vehicles without disruptions or data transfer issues, is addressed by some of the surveyed papers, as detailed in Table 2.9 and Table 2.10.

Complexity is a critical aspect, and it's important to evaluate the time complexity for trust computation and dissemination in Vehicular Networks. Some surveyed approaches introduce delays in the calculation of direct trust, which can be problematic in the context of the Internet of Vehicles (IoV). In scenarios with network density and potential attackers, the detection rate of malicious nodes may decrease due to the network's high density. This underscores the need for efficient and timely trust value determination.

Communication overhead, which measures the amount of transmitted data, also plays a crucial role in the evaluation of these approaches. High communication overhead can lead to inefficient network performance, increased bandwidth consumption, response time delays, and other issues. While some schemes achieve a reasonable forwarding rate even with a higher number of malicious nodes, a few surveyed approaches should pay more attention to managing communication overhead, especially when integrating multiple technologies.

Efficiency is a paramount criterion when assessing trust management schemes. A highly efficient system not only ensures network security but also exhibits resilience against a variety of common security attacks. Within this survey, schemes are considered efficient when they demonstrate resistance to multiple prevalent security attack types, highlighting their robustness and reliability in the face of potential threats. This efficiency is crucial for maintaining the integrity and trustworthiness of network systems.

Based on the findings in Table 2.9 and Table 2.10, it's evident that most of the approaches utilizing emerging technologies are indeed efficient and capable of withstanding common security attacks.

## 2.7 Future Work

In this section, we delve into key challenges and potential avenues for future research in the realm of trust management within Vehicular Networks. Specifically, we highlight the following areas : solutions based on Federated Learning, the use of Clustering methodologies, the impact of energy consumption, and the integration of emerging technologies.

### 2.7.1 Federated Learning-based solutions

The integration of Artificial Intelligence-driven techniques into trust management within Vehicular Networks significantly enhances network efficiency. One noteworthy example is Federated Learning (FL), which is a decentralized Machine Learning approach discussed in reference [112]. FL effectively addresses concerns associated with centralized training by allowing all network participants to contribute to the development of a global model without the need to directly share their data.

In Vehicular Networks, participant nodes often exhibit distinct roles and characteristics. This uniqueness makes FL particularly advantageous as it enables the creation of robust trust formulas and models that leverage distributed intelligent methods, encompassing a wide range of parameters and metrics. This diversity not only enhances the adaptability but also the overall effectiveness of trust management within the network.

### 2.7.2 Clustering approaches

The decentralized nature of trust management underscores the importance of adopting a clustering paradigm, as elaborated in reference [113]. This approach assumes a crucial role in enhancing the overall system's reliability. It becomes especially advantageous when integrating emerging and decentralized technologies, such as Software-Defined Networking (SDN) or Blockchain. These advanced technologies make notable contributions to boosting system performance and streamlining the coordination among various Cluster Heads (CH) within the vehicular network.

### 2.7.3 Energy consumption

With each introduction of a new mechanism or technology into Vehicular Networks, there is a notable increase in communication overhead and time complexity. This escalation poses a substantial challenge in meeting the real-time application requirements of these networks. As a result, it becomes imperative for

future researchers to prioritize energy efficiency when developing trust management models. To tackle this challenge effectively, a recommended approach is to focus on implementing lightweight methodologies. These lightweight approaches have the potential to significantly reduce the energy consumption of the system. Not only does this optimization enhance system performance, but it also ensures that Vehicular Networks can readily meet the demands of real-time applications without compromising energy efficiency. This approach is further elaborated in reference [114].

### 2.7.4 Emerging technologies

The integration of emerging technologies such as Cloud Computing, Software-Defined Networking (SDN), Edge/Fog Computing, or Blockchain into trust management within Vehicular Networks holds the potential to significantly enhance system performance. These technologies offer a reliable, dynamic, scalable, and secure approach to trust management. For example, Cloud Computing and SDN pave the way for a scalable, programmable, and flexible system. However, it's essential to continue researching and addressing challenges related to system complexity, time constraints, and communication overhead to fully harness their potential. On the other hand, Fog/Edge Computing provides localized processing capabilities but introduces potential security and privacy vulnerabilities due to its proximity to user identities and sensitive information, such as location and identity. Mitigating these issues is of utmost importance when implementing these technologies. Blockchain technology ensures the secure signing, verification, and resilient storage of all exchanged data, providing traceability. Nonetheless, trust management schemes based on Blockchain may face power consumption challenges during the trust establishment process, mainly due to block and consensus generation delays. These concerns need careful consideration and management in future research and implementation efforts to leverage the benefits of Blockchain while optimizing resource usage.

## 2.8 Conclusion

In this chapter, we have delved into the foundational principles of trust management within Vehicular Networks. Our study's objective is to develop an effective approach to trust management that strikes a harmonious balance between privacy, security, and service quality. Distinguishing our work from previous surveys in this field, we have explored various categories of trust models specifically tailored for Vehicular Networks. Our exploration commenced with an in-depth examination of Intelligent Transportation Systems (ITS) and Vehicular Networks, underscoring the pivotal role of security in this domain. We emphasized the imperative need for trust models to facilitate secure communication in Vehicular Networks. Additionally, we addressed the security and trust management challenges that are intrinsic to these networks, offering insights into security threats and their corresponding solutions. Subsequently, we conducted a survey of existing trust management schemes, categorizing them as entity-based, data-based, or hybrid models. Furthermore, we introduced our own taxonomy, which encompasses the integration of Artificial Intelligence techniques (including Clustering and Reinforcement Learning, Fuzzy Logic, Game Theory) and emerging technologies (such as Cloud Computing, Software-Defined Networking, Fog/Edge Computing, and Blockchain). Following this survey, we provided a summary of the assessed schemes based on predefined criteria, and subsequently, a qualitative comparison was presented. Our work concluded with an exploration of four emerging research directions, including Federated Learning-based trust approaches, clustering methodologies, considerations for energy efficiency, and the influence of deploying emerging technologies on trust models. In this context, we took into account aspects like scalability, computational overhead, and time complexity.

CHAPITRE 3

# PREDICTION AND DETECTION OF DDOS ATTACKS IN SDVN

## Table des matières


3.1 Introduction . . . . . 58
3.2 A Robust SDVN Framework for Mitigating DDoS Attacks . . . . . 58
3.2.1 Brief Overview . . . . . 58
3.2.2 Proposed work . . . . . 59
3.3 Proposed model's performance . . . . . 60
3.4 Evaluation . . . . . 63
3.5 Discussions . . . . . 66
3.6 Conclusion . . . . . 67

## 3.1 Introduction

Within the realm of Smart Cities, Vehicular Networks stand as the intersection of Intelligent Transportation Systems (ITS) and wireless communication technologies. These networks fall under the category of Mobile Ad-Hoc Networks (MANETs), possessing unique characteristics and requirements specific to vehicular nodes, as elucidated in reference [115].

The dynamism of vehicular networks is exceptional, propelled by the swift movement of network nodes, namely vehicles, resulting in a perpetually changing network topology. The integration of Software-Defined Networking (SDN) in Vehicular Networks (SDVN) introduces challenges, notably congestion on the control-data communication channel and management overhead on the controller. The continuous evolution of the network topology poses difficulties in maintaining an up-to-date global network view at the controller. Furthermore, the decentralized nature of Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communication protocols may not seamlessly align with the SDN global view, necessitating substantial protocol redesign.

Moreover, the application of security and communication solutions from traditional SDN to SDVN is intricate due to the differing characteristics of the two. While SDN relies on static switches and routers, SDVN involves SDN-enabled Base Stations (BSs) and mobile vehicles, as detailed in reference [122]. The control plane elements also vary, with SDN utilizing dedicated server machines as controllers, while SDVN's control plane comprises servers, Roadside Units (RSU), and RSU Controllers (RSUC), each supporting various functionalities. Privacy considerations differ as well, with SDN systems generally offering higher privacy compared to SDVN, which interacts closely with drivers' location information and exhibits high mobility. The data plane in SDVN consists of vehicular devices facilitating multi-hop data forwarding, posing a challenge for the controller in maintaining an up-to-date global view due to the mobility of vehicular nodes.

Vehicular networks face susceptibility to various security issues inherent in wireless communication. Safeguarding these networks is crucial, with Distributed Denial of Service (DDoS) attacks, as discussed in reference [121], emerging as a rapidly growing concern. A successful DDoS attack in Vehicular networks can lead to severe consequences, including accidents and loss of life. Cisco predicts a doubling of the total number of DDoS attacks to 15.4 million by 2023, as mentioned in reference [123].

In SDVN, DDoS attacks aim to flood the bandwidth of the control plane, OpenFlow switches, and the SDN controller (SDNC). Multiple attackers generate numerous new flows with spoofed IP addresses, overwhelming the switch's flow rules and resulting in a flood of packet-in messages sent to the SDNC. This consumes communication resources in both the control and data planes, affecting bandwidth, memory, and CPU usage. OpenFlow switches, under such attacks, accumulate received messages before sending them to the SDNC, leading to increased bandwidth consumption and longer delays in installing new flow rules.

In response to these challenges and security threats, this chapter proposes an anomaly detection and classification approach for SDVN. The approach incorporates a predictive, detection, and security mitigation model to enhance the security and reliability of Vehicular networks. This proactive strategy aims to address the evolving dynamics and unique vulnerabilities of SDVN, providing a foundation for a more resilient and secure vehicular communication infrastructure.

## 3.2 A Robust SDVN Framework for Mitigating DDoS Attacks

In this section, we outline the hierarchical architecture we have proposed for enhancing the security of SDN-based Vehicular Networks. Subsequently, we introduce the key components of our security model, which are dedicated to the prediction, detection, and mitigation of Distributed Denial of Service (DDoS) attacks in SDVN.

### 3.2.1 Brief Overview

Figure 3.1 provides an overview of our hierarchical Software-Defined Vehicular Network (SDVN) architecture, which is structured into three key layers : the Data layer, the SDN layer, and the Cloud layer. The Data layer comprises a diverse array of nodes, both static and dynamic, actively involved in real-time data collection. The primary purpose of this layer is to transmit collected data to the SDN layer. These nodes come in various forms, including connected vehicles, Roadside Units (RSUs), and Base Stations (BSs). It's worth noting that vehicles operating within the SDVN framework, as described in reference [130], are equipped with multiple network interfaces. This dual-access capability enables them

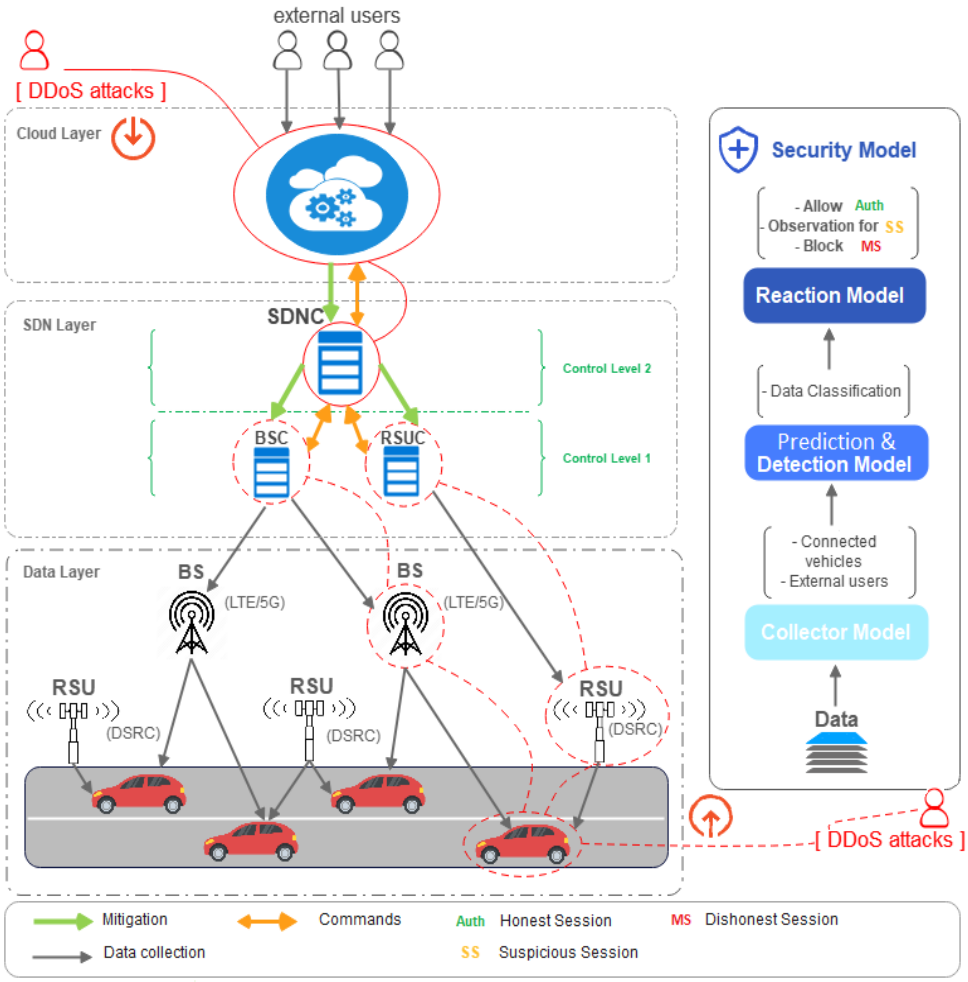



FIGURE 3.1 – Security model for hierarchical SDVN architecture.

to connect to both the RSUs network using Dedicated Short Range Communication (DSRC) and the cellular network (LTE/5G). The SDN layer is further divided into two control levels :

— Control level 1 comprises local controllers, specifically the Roadside Units Controller (RSUC) and the Base Stations Controller (BSC).

— Control level 2 is governed by the principal controller of the architecture, the SDN controller (SDNC).

The SDN layer serves as the central hub for processing and scrutinizing the submitted data, effectively harnessing Software-Defined Networking (SDN) features to address the multifaceted demands of Vehicular Networks. These demands encompass challenges related to scalability, latency, network heterogeneity, high mobility, low communication overhead, and the necessity for high throughput.

The Cloud layer is responsible for managing and efficiently processing substantial volumes of data, playing a pivotal role in mitigating Distributed Denial of Service (DDoS) attacks within SDVN architectures. To achieve this objective, we introduce three sub-models : the collector model, the prediction and detection model, and the reaction model, as elucidated in Figure 2. These sub-models collectively bolster the network's security and fortify its threat detection capabilities.

### 3.2.2 Proposed work

In this section, we delve into the specifics of our security model, which is comprised of three distinct sub-models designed to safeguard the SDVN architecture from Distributed Denial of Service (DDoS) attacks.

#### 3.2.2.1 Collector model

The Data Layer includes both Base Stations (BSs) and Roadside Units (RSUs), which play a crucial role in monitoring the vehicles connected to the network. Their responsibilities include collecting all the

data exchanged with the vehicles, and they utilize Dedicated Short-Range Communications (DSRC) or 5G/LTE communication protocols for this purpose. In our study, we've implemented the collector model, which employs the SFlow protocol to collect all incoming data. This encompasses data from external users accessing the Software-Defined Networking Controller (SDNC) through the cloud servers, as well as data transmitted from the vehicles within the Data Layer to the initial control level in the Software-Defined Networking (SDN) infrastructure.

#### 3.2.2.2 Prediction and Detection model

In this module, we conduct an in-depth analysis and categorization of collected data into five distinct statuses to gain insights into the nature of each session. These statuses encompass "Authentic" (Auth) for sessions characterized by minimal activity, "Lightly Suspicious" (LS) for those exhibiting moderate activity, and "Heavily Suspicious" (HS) for sessions with heightened activity, potentially indicative of malicious intent. Furthermore, "Lightly Malicious" (LM) and "Heavily Malicious" (HM) statuses are specifically assigned to sessions demonstrating various degrees of malicious behavior. This classification framework plays a pivotal role in distinguishing between benign, suspicious, and potentially harmful activities, thereby bolstering the effectiveness of network security and threat detection measures.

#### 3.2.2.3 Reaction model

In this module, we have implemented a reaction algorithm aimed at mitigating the attacks identified through the prediction and detection model, taking into account the status of each session. Honest sessions, corresponding to authentic nodes in the network, are recognized and rewarded with increased bandwidth allocation as part of our incentive mechanism. On the other hand, dishonest sessions or Heavily Malicious nodes are promptly blocked to prevent further harm. For sessions categorized as suspicious, which includes both Lightly and Heavily Suspicious sessions, they are initially treated as potentially malicious sessions. However, we refrain from immediate action within a specific time slot denoted as $T_{slot}$. Instead, we initiate a deeper investigation and observation period. During this time, a suspicious node may undergo a change in status, transitioning to either an honest/authentic and allowed node or a dishonest and blocked node, depending on its behavior and compliance with the reaction algorithm. This approach allows us to make well-informed decisions regarding the status of suspicious nodes, promoting an adaptive and dynamic network security response.

**Algorithm 1:** Reaction algorithm

```
SessionStatus ← none;
behavior ← none;
th ← t;
if LOG.size ≠ th1 then
    SessionStatus ← Auth;
if LOG.size ≥ th4 then
    SessionStatus ← Block;
if (LOG.size > th1) (LOG.size ≤ th3) then
    behavior ← malicious;
    while T_slot ≠ 0 do
        observation ← observ;
        if observation = abnormal then
            behavior ← malicious;
            SessionStatus ← Block;
        if observation = normal then
            behavior ← authentic;
            SessionStatus ← Auth;
```

## 3.3 Proposed model's performance

In this section, we introduce our stochastic security model designed for the detection of DDoS attacks based on device behavior analysis. The model goes a step further by predicting the future state of devices

using a Markov chain model and a stochastic transition probability matrix. In this study, we employ a Markov stochastic process to examine the behavior of individual devices. Leveraging log data, we delineate distinct behavior ranges by applying different thresholds, thereby enabling the characterization of each device. This categorization helps identify the source of the behavior, whether it originates from external users or connected vehicles within the Data plane, as illustrated in Figure **??** The primary objective of this chapter is to mitigate DDoS attacks, which typically involve flooding the system, as discussed in Section 1 and illustrated in the accompanying figure.

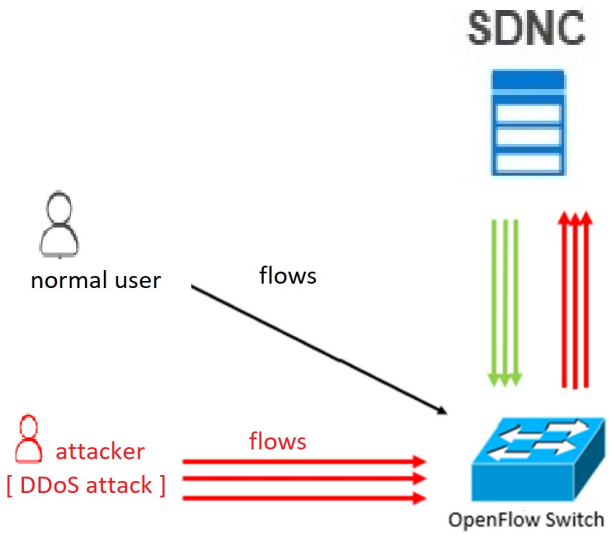



FIGURE 3.2 – OpenFlow Switch under DDoS attack.

We categorize security attacks into two types : "lightly malicious" and "heavily malicious." Lightly malicious attacks may occur accidentally due to a mishandling device, whereas heavily malicious attacks are deliberate actions carried out by malicious devices. Our stochastic model is designed to identify the device's state based on the number of recorded activities in the log. To achieve this, we employ a session-behavior ranges mechanism, as depicted in Figure 3.3 . We classify sessions into five distinct ranges :

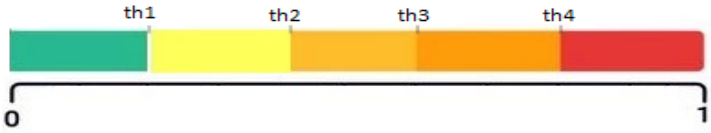



FIGURE 3.3 – Behavior ranges thresholds

Authentic, Lightly Suspicious, Heavily Suspicious, Lightly Malicious, and Heavily Malicious, using four fixed threshold values : th1, th2, th3, and th4. These thresholds enable us to determine the state of each session. For example, a session initially categorized as Heavily Suspicious at the beginning of a Time Slot $T_{slot}$ can transition to the Heavily Malicious state if the number of reported activities exceeds the threshold th4. In this study, we present seven possible states, as listed below :

- The "Authentic state" (Auth) is defined as the state where the device's log size is lower than the threshold th1.
- The "Lightly Suspicious state" (LS) is characterized by the device's log size falling between the threshold th1 and th2.
- The "Heavily Suspicious state" (HS) occurs when the device's log size falls between the threshold th2 and th3.
- The "Lightly Malicious state" (LM) is indicated when the device's log size falls between the threshold th3 and th4.
- The "Heavily Malicious state" (HM) is identified when the device's log size exceeds the threshold th4.
- The "Block state" is activated once an attack has occurred and the session is blocked as a security measure.
- The "Observation state" (Observ) is characterized by the device's log size falling between the threshold th2 and th4. In this state, only nodes classified as authentic will be directly allowed, while all other nodes will be observed for a specific time slot, as outlined in Algorithm 1.

$$\lambda_{id,i}(t) = p\{v_{id,t} = i\}. \tag{3.5}$$

$$\{\lambda_{id,HM}(t+1), \lambda_{id,LM}(t+1), \lambda_{id,HS}(t+1), \lambda_{id,LS}(t+1), \lambda_{id,Auth}(t+1)\} = \{\lambda_{id,HM}(t), \lambda_{id,LM}(t), \lambda_{id,HS}(t), \lambda_{id,LS}(t), \lambda_{id,Auth}(t) * M_{p_{id}}\}. \tag{3.6}$$

In this system, each session has the capability to transition from one state to another, which is referred to as a transition process, as depicted in Figure 3. We define the state space of potential states for each vehicle, denoted as "S," where S = Auth, LS, HS, LM, HM, Observ, Block. The network's evolution is represented by a semi-Markov process. Therefore, the state of the network is a union of the states of all vehicles, where $v_{id}{}^{t}$ represents the state of the vehicle identified by an id at time t, and $V_t$ denotes all the vehicles' states at time t. This relationship can be expressed using the following equation :

$$V_t = \bigcup_{id=1}^{n} v_i d^t \tag{3.1}$$

Furthermore, it's important to note that the state of a node is memory-less, signifying that the present, past, and future states are independent. Therefore, the state of a node at a future time (t+1) is solely determined by its state at the current time t and is not influenced by its past state at time (t-1). To depict the evolution of a vehicle's behavior identified by id over time, we employ a stochastic state transition matrix. This matrix contains transition probabilities between two states based on behavior range thresholds as depicted in Figure 4. The equation is as follows :

$$P_{id,i\to j} = p(v_{id,t+1} = j | v_{id=i} = i) = p(v_{id,1} = j | v_{id,0} = i). \tag{3.2}$$

Where $P_{i\ j}$ denotes the transition probability of a vehicle from state i to state j.
The evolution over time of a vehicle identified by an id is represented by a matrix $M^{t}{}_{P_{id}}$ shown as follows.

$$M^{t}{}_{P_{id}} = \begin{bmatrix} P_{id,HM\to HM} & P_{id,HM\to LM} & P_{id,HM\to HS} & P_{id,HM\to LS} & P_{id,HM\to Auth} \\ P_{id,LM\to HM} & P_{id,LM\to LM} & P_{id,LM\to HS} & P_{id,LM\to LS} & P_{id,LM\to Auth} \\ P_{id,HS\to HM} & P_{id,HS\to LM} & P_{id,HS\to HS} & P_{id,HS\to LS} & P_{id,HS\to Auth} \\ P_{id,LS\to HM} & P_{id,LS\to LM} & P_{id,LS\to HS} & P_{id,LS\to LS} & P_{id,LS\to Auth} \\ P_{id,Auth\to HM} & P_{id,Auth\to LM} & P_{id,Auth\to HS} & P_{id,Auth\to LS} & P_{id,Auth\to Auth} \end{bmatrix}$$

It is composed by the probabilities of transition between other states where $P_{id}$=$P_{id,i\ j}$ and {i,j$\in S$}.
In $M_{P_{id}}$, the sum of each row probabilities must be equal to 1. We can present the equation as follows :

$$\sum_{j=\{Auth,LS,HS,LM,HM\}} P_{id,i\to j} = 1. \tag{3.3}$$

The transition probability, denoted as $\alpha_{i\to j}$, is defined as the fraction of the number of transitions of a node from its current state i to another state j, divided by the expected number of visits to state i, referred to as $\beta_{i\to j}$.

The calculation of the transition probability is determined by the following equation :

$$P_{id,i\to j} = p(v_{id,t+1} = j | \cup_{id=1}^{n} v_{id,t} = i) = \frac{\alpha_{i\to j}}{\beta_{i\to j}} \tag{3.4}$$

We assess the behavior of each vehicle based on its progression after determining the state in our Markov chain. Therefore, at time t, the probability of a vehicle identified by an id being in state i, denoted as $\lambda_{id,i}$(t), is determined using the following equation :

Furthermore, we can represent the stochastic vector $V_{\lambda_{id}(t)}$ at any given time t using the equation as follows : Hence,

$$V_{\lambda_{id}}(t+1) = V_{\lambda_{id}(t)} * M_{p_{id}}. \tag{3.7}$$

Our vehicle behavior Markov chain is defined by its transition matrix $M_{P_{id}.Therefore,}\lambda_{id}(0)$ represents the initial transition probabilities of our Markov chain over n steps. It has at least one stationary probability distribution, which is determined by the following equation :

$$\lim \lambda_{id}(n). \tag{3.8}$$

The Markov process is a stochastic process that involves a sequence of random states with associated transition probabilities. In our transition diagram, illustrated in Figure 3, we depict five distinct states for a single vehicle. For example, there are no transitions from the "Block" state to any other state. This is referred to as an absorbing or absorbing state, indicating that once a node enters this state, it cannot change its state. The Markov process is in an alert mode, signifying that an attack is in progress, and the system must take measures to mitigate the risk and promptly issue an intrusion alert. In contrast, all the other states within the diagram are considered transitioning states, indicating that nodes can move between these states as part of the dynamic Markov process.

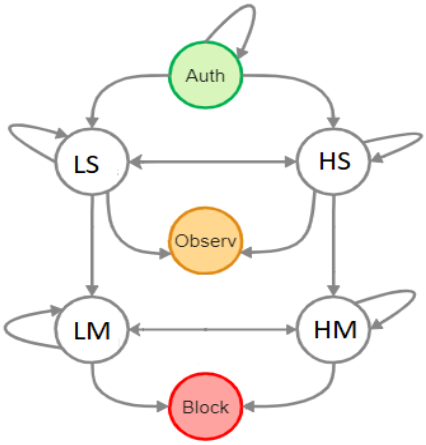



FIGURE 3.4 – Behavior ranges thresholds

## 3.4 Evaluation

In this section, we outline the evaluation parameters that illustrate the effectiveness of our approach in detecting and predicting malicious nodes with the intention of thwarting DDoS attacks, particularly those aimed at flooding the flow tables of OpenFlow Switches.

We conducted simulations of our solution using MATLAB, considering a range of scenarios as presented in Table.2. In these simulations, we predicted the behavior of each network node based on a stochastic Discrete Time Markov Chain process.

To assess the classification performance of our model, we subjected our network to diverse conditions. Additionally, we varied the network size, encompassing scenarios with 20, 60, 80, and 100 vehicles, while also adjusting the proportions of lightly malicious (LM) and heavily malicious (HM) nodes. Specifically, we examined five cases : 5% (3% HM + 2% LM), 10% (6% HM + 4% LM), 15% (9% HM + 6% LM), 20% (12% HM + 8% LM), and 25% (15% HM + 10% LM), which are detailed in Table.2. In these evaluations, we maintained fixed threshold values : 0.25 for th1, 0.45 for th2, 0.65 for th3, and 0.75 for th4.

To illustrate our work's evaluation, we present a specific case involving a network comprising 100 nodes at time t without applying the Markov process, as depicted in Figure.6. In this case, the network configuration consisted of 3% Heavily Malicious nodes, 2% Lightly Malicious nodes, 10% Lightly Suspicious nodes, 10% Heavily Suspicious nodes, and 75% Authentic nodes.

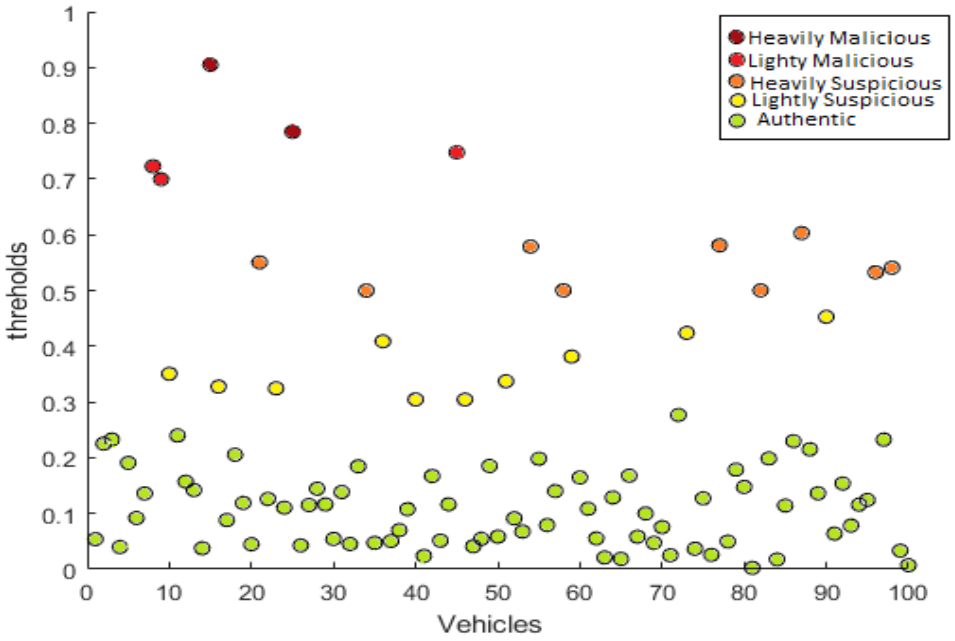



FIGURE 3.5 – The distribution of vehicles at time t.

TABLE 3.1 – Repartition of nodes in the network.

| Case | Auth | LS | HS | LM | HM |
|---|---|---|---|---|---|
| Case I | 75% | 10% | 10% | 2% | 3% |
| Case II | 70% | 10% | 10% | 4% | 6% |
| Case III | 65% | 10% | 10% | 6% | 9% |
| Case IV | 60% | 10% | 10% | 8% | 12% |
| Case V | 55% | 10% | 10% | 10% | 15% |

We evaluate the performance of our model by calculating the reliability. The equation is mentioned below :

$$Reliability = \frac{R_{\mathrm{TP}} + R_{\mathrm{TN}}}{Nbe_{\mathrm{Total,Vehicle}}} \tag{3.9}$$

$$Unreliability = \frac{R_{\mathrm{FP}} + R_{\mathrm{FN}}}{Nbe_{\mathrm{Total,Vehicle}}} \tag{3.10}$$

Where $R_{TP}$,$R_{FP}$, $R_{TN}$, $R_{FN}$ and $Nbe_{Total,Vehicle}$ are determined as follows :

- $R_{TP}$ : The True Positive Rate refers to the accurate classification of honest nodes, indicating the proportion of genuine nodes correctly identified.
- $R_{FP}$ : The False Positive Rate signifies the misclassification of honest nodes, representing the count of genuine nodes erroneously identified as something else.
- $R_{TN}$ : The True Negative Rate denotes the accurate classification of malicious nodes, representing the count of harmful nodes correctly identified.
- $R_{FN}$ : The False Negative Rate pertains to the misclassification of malicious nodes, indicating the quantity of harmful nodes erroneously identified as something other than malicious.
- $Nbe_{Total,Vehicle}$ : The total number of vehicles.

Using MATLAB, we conducted multiple simulations to assess our work's performance under various conditions at different time instances, specifically at time t, t+1, t+2, t+3, and t+4, with t representing

the initial moment within the network. These simulations and their outcomes are depicted in Figures 3.5 to 3.10. For our network, we considered a total of 20 nodes and adopted Case V from Table 2. In this configuration, 25% of the nodes were designated as malicious, comprising 15% Heavily Malicious (HM) nodes and 10% Lightly Malicious (LM) nodes, while 10% were Low Security (LS), 10% High Security (HS), and the remaining 55% were identified as authentic nodes. Utilizing Equation 3.4, we calculated the transition probabilities ($P_{id,i\to j}$) for each node, specifying the likelihood of a node with ID "id" transitioning from state "i" to state "j." Our simulations reveal that vehicles initially classified as Heavily Malicious or Lightly Malicious at time instances t, t+1, t+2, t+3, and t+4 tend to maintain their malicious state. On the other hand, Vehicle ID = 1 consistently retains its authentic status, maintaining its initial state from t to t+4. Consequently, this particular vehicle is deemed typical and should be rewarded with increased bandwidth allocation. The primary objective of this research is to predict the future states of network nodes. Calculations based on Equation 3.9 and Equation 3.10 indicate that the reliability of the system increases to 80%, while the unreliability rate remains at 20%.

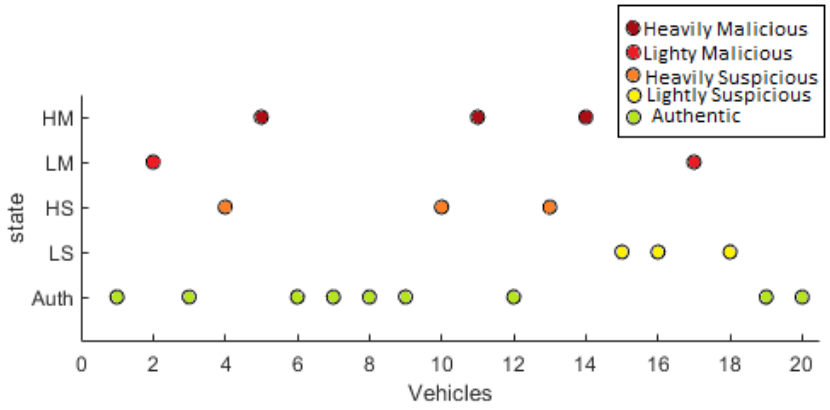



FIGURE 3.6 – The distribution of vehicles at time t.

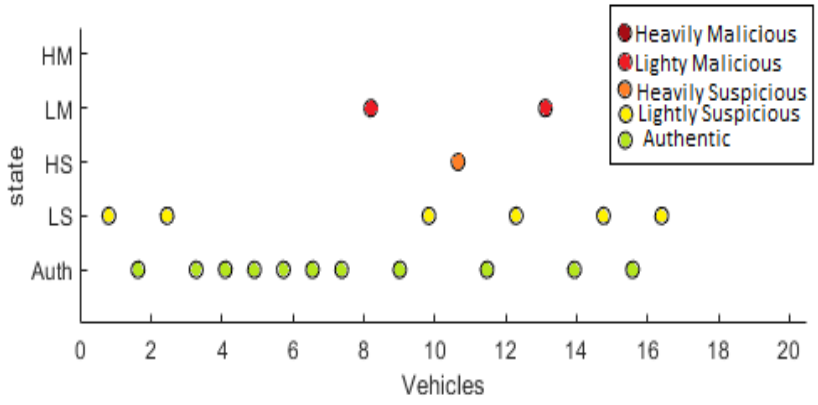



FIGURE 3.7 – The distribution of vehicles at time t+1.

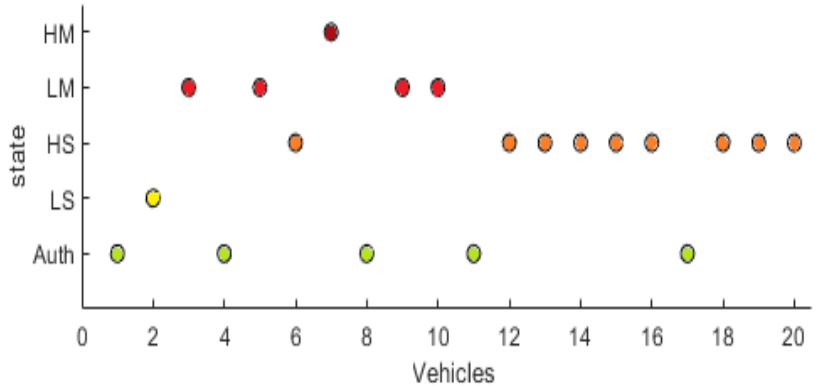



FIGURE 3.8 – The distribution of vehicles at time t+2.

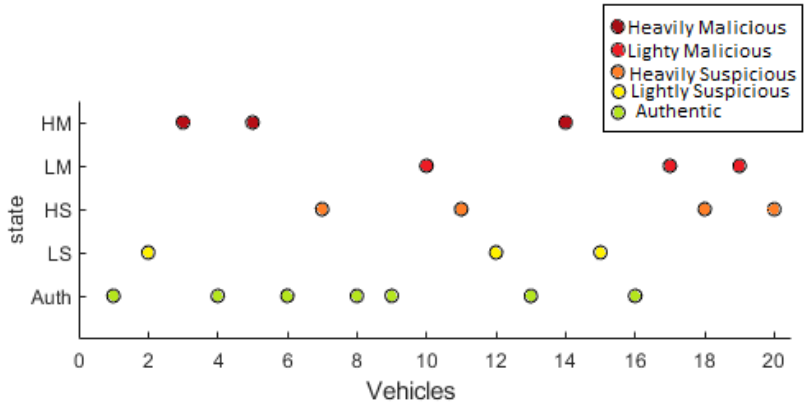



FIGURE 3.9 – The distribution of vehicles at time t+3.

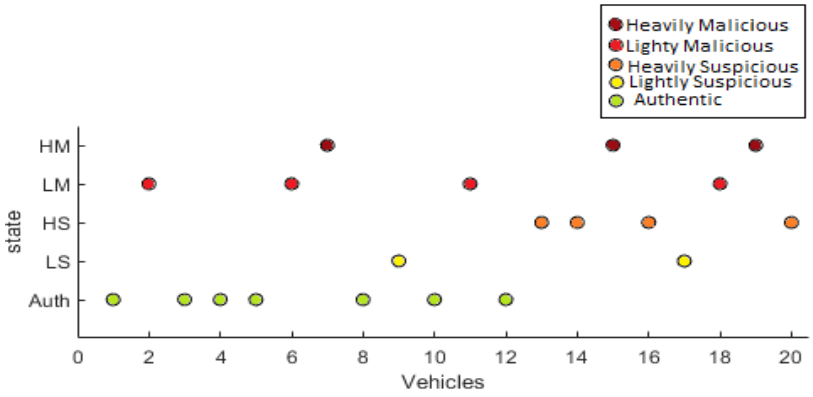



FIGURE 3.10 – The distribution of vehicles at time t+4.

## 3.5 Discussions

In our quest to detect, predict, and mitigate DDoS attacks in vehicular networks, we put forward a secure hierarchical Software-Defined Vehicular Network (SDVN) architecture. This architecture empowers the design of flexible and programmable networks. Our approach involves the development of a security model designed to proactively identify and anticipate future attacks. This is achieved through the utilization of proposed algorithms and a stochastic Markov process. The ultimate goal is to preemptively identify and block malicious nodes before they can instigate attacks within the system. To accomplish this, we employ fixed and well-defined threshold values to categorize the network's nodes into specific

states. Through extensive simulations conducted under various conditions, our model demonstrates a high reliability rate of 80% and a 20% unreliability rate.

## 3.6 Conclusion

In this chapter, a secure hierarchical architecture for Software-Defined Vehicular Networks (SDVN) is introduced with the primary objective of mitigating Distributed Denial of Service (DDoS) attacks, leveraging a mathematical Markov model. The proposed architecture is structured into three layers : the Data layer, the SDN layer, and the Cloud layer. The security model is composed of three distinct sub-models : the Collector model, the Prediction and Detection model, and the Reaction model. This contribution delves into a detailed exposition of the stochastic Markov model employed for prediction and detection. An evaluation was conducted using MATLAB to scrutinize the behavior of network nodes, predicting their future states based on their current conditions.

The outcomes of our evaluation affirm the lightweight nature of our solution, showcasing a commendable detection rate of up to 80%. This efficiency is achieved by leveraging probability and analytical formulas inherent in the Discrete Time Markov chain model, facilitating swift mitigation. As part of our future research endeavors, we aim to implement a dynamic method for determining thresholds. Our strategy for predicting attacks relies on the Markov process, utilizing the current state of the node. This approach offers a lightweight solution with minimal computational complexity, thus avoiding potential drawbacks associated with a lower detection rate. The model can be implemented either within the SDN layer or the data plane layer. In our contribution, we have instantiated it within the SDN layer to identify attacks originating from external users traversing Cloud servers or from connected nodes via control level 2 entities, as illustrated in Figure 1.3.

CHAPITRE 4

# TRUST MANAGEMENT FOR CONNECTED VEHICLES WITH PRIVACY PRESERVING

## Table des matières


4.1 Introduction . . . 70
4.2 System model . . . 70
4.2.1 Proposed Blockchain . . . 72
4.2.2 Network Components . . . 73
4.3 Adversary model . . . 73
4.3.1 Adversary RSU . . . 73
4.3.2 Adversary vehicles . . . 75
4.4 Vehicles' Pseudonyms Management . . . 75
4.4.1 System initialization (SDNC, RSUC, Vehicles) . . . 75
4.4.2 Vehicles' and RSUCs' registration . . . 75
4.4.3 Vehicle authentication . . . 76
4.4.4 Message authentication . . . 77
4.5 Trust Model . . . 78
4.5.1 Trust system's process . . . 78
4.5.2 Trust Process . . . 79
4.6 Implementation . . . 80
4.7 Security analysis . . . 81
4.8 Conclusion . . . 82

## 4.1 Introduction

The exponential growth of connected vehicles within modern transportation systems has ushered in a transformative era of mobility. These interconnected automobiles promise unparalleled convenience, efficiency, and safety. The exponential growth of connected vehicles in modern transportation systems has indeed marked a transformative era in mobility. These vehicles, equipped with advanced communication technologies and data-driven capabilities, are reshaping the way we perceive and experience transportation. Connected vehicles are indeed a pivotal enabler for Intelligent Transportation Systems and bring several benefits, such as enhanced safety through real-time communication to avoid accidents, optimized traffic flow, and reduced congestion. They also offer convenience with features like predictive maintenance, automated parking, and in-car entertainment systems. Moreover, connected vehicles play a pivotal role in the development of autonomous driving, promising a future where vehicles can navigate and make decisions based on a vast network of shared data. However, with these benefits come new challenges that must be addressed to ensure the continued success of connected vehicles. First and foremost, trust is a critical concern. As vehicles communicate with each other, infrastructure, and external services, they rely on data and information exchange. Ensuring the authenticity, reliability, and security of this data is paramount. Trust in the sources of information, such as other vehicles and infrastructure components, becomes a central issue in maintaining a safe and efficient connected vehicle ecosystem. According to the World Health Organization every year, over 1.35 million road users are killed on the roads. Trust management system allows vehicles to determine whether the received message is trustworthy or not, and also equips network operators with the basis of rewards or punishments on specific vehicles. Security is another pivotal aspect. The interconnected nature of these vehicles makes them susceptible to cyber threats and malicious attacks. Unauthorized access, data breaches, and the potential for cyber-physical attacks pose significant risks. Therefore, robust security measures are essential to protect both the vehicles and their passengers. Data integrity is yet another challenge. connected vehicles generate and rely on vast amounts of data, from sensor readings to real-time traffic information. Ensuring that this data remains accurate and untampered with is vital for the proper functioning of various applications, including autonomous driving and traffic management. In response to the evolving landscape ; cited in the introduction ; of connected vehicles and the imperative need for secure ITS, several trust-based mechanisms have been introduced. These mechanisms are meticulously designed to address the multifaceted challenges associated with the seamless and secure integration of vehicles into an interconnected network. These mechanisms include (1) Public Key Infrastructure (PKI) : PKI is a widely adopted trust mechanism that employs asymmetric cryptography. It involves the use of digital certificates to verify the identity of entities within the vehicular network. Vehicles and infrastructure components possess unique digital certificates, allowing for secure communication and authentication. PKI is fundamental for establishing trust in the authenticity of messages and participants ; and (2) Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Communication Protocols : These mechanisms define the rules and standards for secure communication between vehicles and infrastructure. Protocols like IEEE 802.11p (Wireless Access in Vehicular Environments, WAVE) ensure that messages exchanged are encrypted, signed, and authenticated, preventing unauthorized access and message tampering.

However, these solutions suffer from several limitations including, a lack of flexibility, transparency, and efficiency. These limitations extend to various facets, including the lack of (1) flexibility : Existing trust management systems often struggle to adapt swiftly to the ever-changing dynamics of Vehicular networks. The fluid nature of ITS necessitates trust mechanisms that can swiftly re-calibrate to accommodate shifting trust requirements. Rigid systems can lead to security gaps as they may not respond adequately to emerging threats or changing network conditions ; (2) transparency Gaps : Many of these solutions operate within a veil of opacity, leaving stakeholders in the dark regarding the decision-making processes that govern trust. This lack of transparency can undermine confidence among participants, hindering effective collaboration and impeding the identification of anomalies or vulnerabilities ; and (3) Centralization Perils : Perhaps the most critical drawback lies in the reliance on centralized trust authorities for the exchange of security certificates and keys. This centralized approach, while convenient, introduces a perilous single point of failure. In the event of a breach or failure at this central juncture, the entire trust infrastructure becomes vulnerable, culminating in a cascading failure that can jeopardize the integrity and security of the entire ITS ecosystem.

## 4.2 System model

In this section, we describe our proposed system model. It aims to develop a decentralized trust management system in SDVN with privacy-preserving. We start by introducing the network components.

Then, we describe our Blockchain-based framework. The network components encompass the Trusted Authority (TA), Roadside Unit Controller (RSUC), and the ensemble of connected vehicles.

#### 4.2.0.1 Trusted Authority (TA) :

The Trusted Authority (TA) assumes the pivotal role of facilitating the initial registration of vehicles within the network. Consequently, it leverages a private Blockchain to oversee the transactions associated with the first authentication. These transactions encapsulate essential vehicle information at the time of their inaugural network entry. Following this initial registration phase, vehicles cease direct communication with the TA, effectively diminishing reliance on it. As a consequence, this approach significantly reduces the dependency on the TA. Notably, within this framework, only Roadside Unit Controllers (RSUCs) are granted access to this information, thereby enabling them to verify the authenticity of specific vehicles.

#### 4.2.0.2 Road Side Unit Controller (RSUC) :

RSUCs and RSU have potential resources that make them able to perform heavy tasks in the network such as managing the pseudonyms of vehicles, and collecting ratings and trust values. We describe these tasks as follows :

— **Collecting Pseudonyms :** Pseudonyms generated by the vehicles are stored and managed by the RSUC.
— **Collecting Ratings :** We assume that only RSUCs are responsible for collecting the ratings uploaded by the vehicles. The vehicles are equipped with limited OBUs that can not deal with a large amount of exchanged data locally in the long term. Therefore, the message receivers will only generate the ratings' values to evaluate the credibility of the messages and upload them directly to the relevant RSUC, where they will be collected and stored in the long term. However, they must be periodically updated by vehicles.

— **Managing trust values :** Based on the generated ratings' values, the vehicles' trust values are computed depending on the RSUC's qualifications. The trust value measure is based on the aggregated opinion of a node, which depends on the credibility of its sent messages. The calculated trust values are stored in the RSUC. Hence, the vehicles will be able to ask for any node's trust value.

#### 4.2.0.3 Connected vehicles

In the Internet of Vehicles, the connected vehicles are equipped with onboard units (OBUs) that assume the responsibility of collecting, processing, and sharing data. This data exchange enables communication with Roadside Units (RSUs) or facilitates direct communication with other vehicles within the network. The OBUs are designed to gather a wide array of information, ranging from vehicle telemetry data like speed, acceleration, and braking patterns to environmental data such as weather conditions and road surface quality. They process this data in real time, making it available for immediate sharing with Roadside Units (RSUs) or for direct communication with neighboring vehicles. This robust data-sharing capability not only facilitates essential safety-related information exchange with RSUs but also empowers vehicles to engage in cooperative maneuvers, such as adaptive cruise control, lane merging, and collision avoidance, by communicating directly with nearby vehicles. The OBUs thus play a pivotal role in enhancing both the safety and efficiency of connected vehicle networks. We describe these tasks as follows :

— **Generating Pseudonyms :** The vehicles create Short-Term Certificates considered as new pseudonyms and define their lifetime.

— **Generating ratings :** The vehicles send warning messages about a specific event using V2V [**?**] communication (e.g., Dedicated Short Range Communication (DSRC) and cellular network communications). Moreover, each vehicle has a reference set which is composed of neighboring vehicles traveling in front within a certain distance with elevated relevance to the safety of the target vehicle. This set is responsible for transmitting alert messages about a probable event to conscious the vehicles. Therefore, the vehicles will not send useless warning messages about an event that has already passed its location. However, the messages sent by the reference set may not always be

trustworthy due to malfunctions or misbehaviors. Therefore, the receiver must identify the credible message after aggregating all sent messages about a specific event. Finally, the receiver vehicle can generate and upload the rating value depending on its credibility using defined formulas such as the majority rule.

### 4.2.1 Proposed Blockchain

Smart contracts are self-contained computer programs executed when predetermined conditions are met. Our proposed framework utilizes multiple smart contracts to establish trust and ensure security in future Software-Defined Vehicular networks (SDVN) in a completely distributed, transparent, secure, tamper-proof, and trustworthy manner.

#### 4.2.1.1 Management Smart Contract (MSC)

The Management Smart Contract (MSC) assumes a critical role in the process of vehicle registration, serving as the cornerstone for registering vehicles within the network. It functions as the central authority responsible for overseeing the onboarding procedure of vehicles onto the Intelligent Transportation System (ITS). This multifaceted responsibility encompasses several key functions : (1) Authenticity Verification : MSC is tasked with verifying the authenticity of each vehicle's identity before granting it access to the network. This verification process ensures that only legitimate and authorized vehicles are permitted to participate in the ITS ; (2) Regulatory Compliance : MSC also plays a pivotal role in ensuring that registered vehicles comply with network regulations and standards. This includes validating that vehicles meet the necessary technical and operational requirements mandated by the network ; (3) Registry Management : MSC maintains and updates a comprehensive registry of authorized vehicles within the system. This registry serves as a trusted and up-to-date record of all vehicles allowed to operate within the network ; (4) Trust Establishment : The accurate and secure management of this registry is essential for establishing trust among network participants. By maintaining a reliable record of authorized vehicles, MSC fosters trust and confidence in the system's integrity.

#### 4.2.1.2 Trust Smart Contract (TSC)

Trust Smart Contract (TSC) : TSC includes (a) a Bayesian Trust Model (see Fig. 1) : TSC continuously evaluates and calculates trust scores for each vehicle based on historical data, interactions, and behavior. It takes into account a myriad of factors, including data integrity, message reliability, and past interactions, to assess the trustworthiness of vehicles dynamically ; and (b) an on-chain Trust Scores : The TSC also encapsulates on-chain scores of trust for vehicles. These on-chain trust scores, calculated by the Bayesian model, are recorded on the blockchain for transparency and auditability. This ensures that trust-related decisions are made based on empirical and verifiable data, bolstering the overall trustworthiness of the system

#### 4.2.1.3 Smart contract for revoking (RSC)

This smart contract is a critical component of the trust management system, responsible for handling the revocation of trust for vehicles that have engaged in malicious activities or have become compromised. It ensures that compromised vehicles are swiftly and effectively isolated from the network, preventing them from participating in further transactions. This revocation mechanism enhances the overall security and trustworthiness of the ITS ecosystem. Thus, the vehicles with a trust value lower than a fixed threshold will be blocked from the network and its pseudo-ID will be added to the banned list. Other vehicles will not communicate with it. In fact, honest vehicles will communicate only with the vehicles with pseudo-ID in the authentic list.

#### 4.2.1.4 Smart contract for access control (ACSC)

This smart contract assumes a critical role in overseeing and regulating access control policies within the vehicular network. Its primary functions involve the definition and enforcement of detailed access controls, specifying which vehicles or entities possess the authorization to access particular resources or services. The ACSC plays a pivotal role in maintaining the security and integrity of the Intelligent Transportation System (ITS) by : (1) Access Policy Definition : The ACSC establishes comprehensive access control policies that outline who is allowed to access specific resources, databases, or services within the network. These policies are designed to align with network security requirements ; (2) Authorization

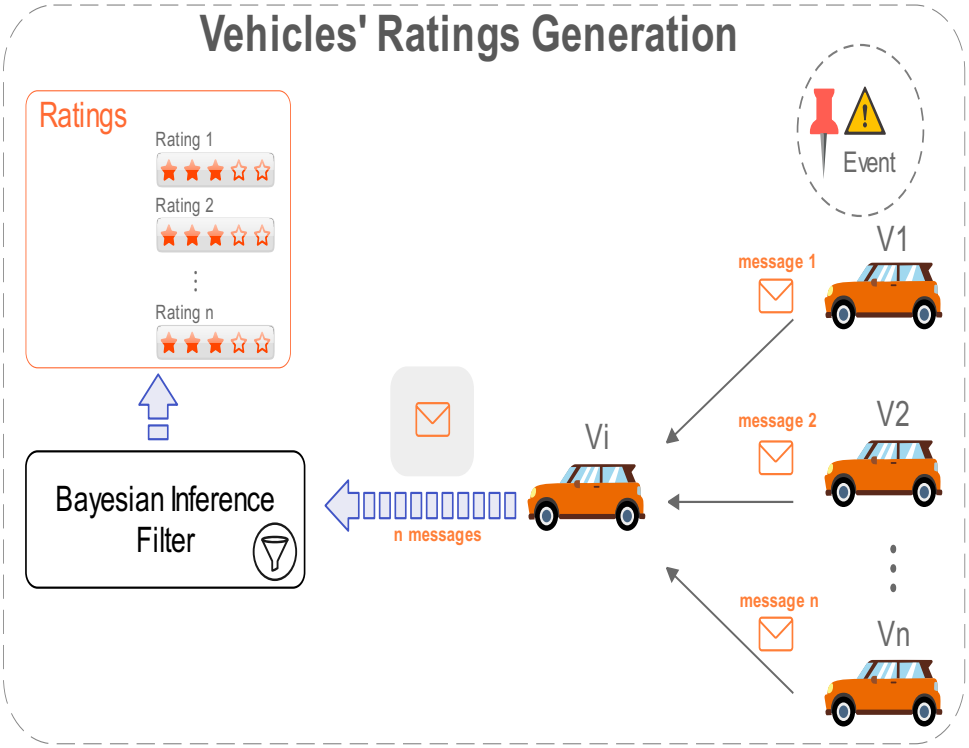



FIGURE 4.1 – Vehicles' ratings generation based on Bayesian Inference Filter.

Enforcement : It actively enforces these access control policies, ensuring that only authorized vehicles or entities can request and access the designated resources. Unauthorized access attempts are systematically prevented ; (3) Security Safeguard : By precisely delineating and enforcing access permissions, the ACSC acts as a robust security safeguard, protecting critical assets, data, and functions within the ITS from potential breaches or misuse ; and (4) Audit Trail : The ACSC can maintain an audit trail of access requests and responses, which can be invaluable for monitoring and analysis, as well as for demonstrating compliance with regulatory requirements.

### 4.2.2 Network Components

## 4.3 Adversary model

In this work, we consider that we have two adversary models : the RSUs and the vehicles. These entities are vulnerable to malicious activities committed by attackers in order to infect the security and privacy of connected vehicles networks.

### 4.3.1 Adversary RSU

Roadside Units (RSUs) serve as stationary infrastructure elements positioned along the road network, and they are known for their substantial computing capabilities. However, it's important to note that RSUs, while having strong computational resources, may sometimes lack robust protection measures, rendering them vulnerable to potential security intrusions. These intrusions could involve unauthorized access, data manipulation, or data deletion. As a result, researchers often classify RSUs as semi-trusted entities within connected vehicle networks. Despite this semi-trusted status, RSUs possess certain advantages over potential malicious nodes in the network. Malicious nodes, even in the case of launching attacks, often operate with limited resources when compared to the substantial computational capacities of RSUs. Additionally, network administrators implement security and privacy checks at regular intervals, which aids in identifying and mitigating potential threats. These periodic security and privacy checks by network administrators make it challenging for attacks to persistently interfere with all compromised RSUs over the long term. While individual RSUs may be targeted and temporarily compromised, the network's resilience, coupled with the periodic checks, helps in mitigating the impact of large-scale attacks and aids in the recovery of compromised RSUs, reinforcing the network's overall security posture.

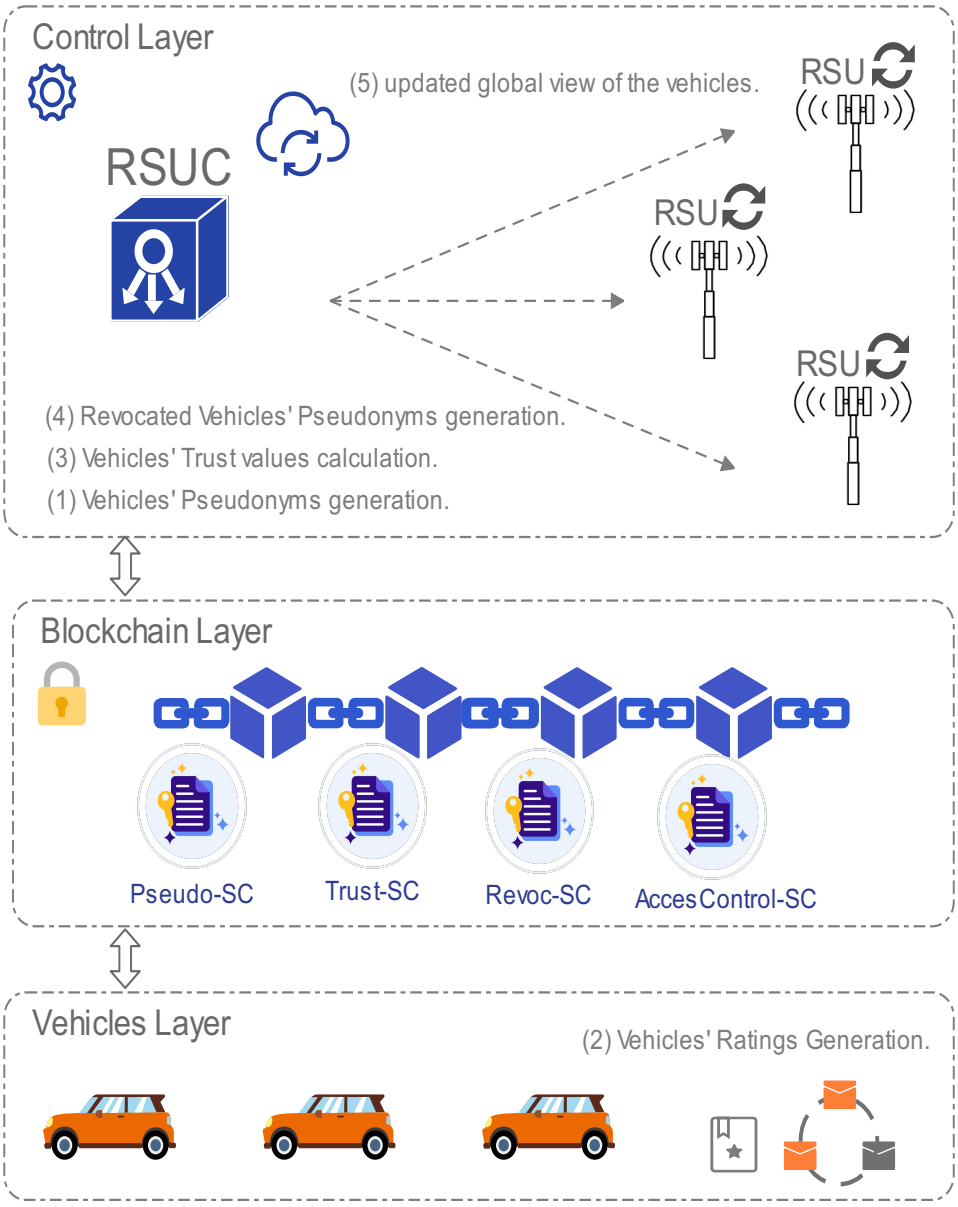



FIGURE 4.2 – System Architecture.

### 4.3.2 Adversary vehicles

Within connected vehicle networks, there exists the possibility of adversary vehicles, which are vehicles within the network that engage in malicious activities with the aim of disrupting the network's normal operation. These adversary vehicles may carry out various nefarious actions, including : (1) Data Interception : Adversary vehicles may attempt to intercept data transmissions within the network, potentially compromising the confidentiality and integrity of the information being exchanged ; (2) Data Manipulation : Compromised vehicles have the capability to alter, add, or delete stored data within the network, which can lead to erroneous information and potentially hazardous situations ; and (3) Deceptive Communication : Adversary vehicles can send deceptive or bogus messages with the intent to mislead honest nodes or other vehicles. This deceptive communication can disrupt the coordination and cooperation among network participants.

The presence of malicious vehicles within the network poses a significant security challenge, as their actions can have adverse effects on the overall functionality of the network. Unaffected vehicles, that are not engaged in malicious activities, may experience disruptions or adverse consequences due to the actions of these misbehaving vehicles. Therefore, it is crucial for connected vehicle networks to implement robust security measures to detect and mitigate the impact of adversary vehicles, ensuring the network's reliability and integrity.

## 4.4 Vehicles' Pseudonyms Management

### 4.4.1 System initialization (SDNC, RSUC, Vehicles)

In our system, we have three participating entities : the TA, RSUCs and n vehicles, where $V_i = \{1, 2, ...n\}$. We implement a Smart Contract for the pseudonyms' management called Pseudo-SC. To initialize the system, the TA defines the primary parameters using the ECC (Elliptic Curve Cryptography) as below :

— TA generates the ECC E, where $E : (y^2 = x^3 + ax + b) \mod p$ where $a, b \in \mathbb{Z}_q^*$ and $(4a^3 + 27b^2) \mod p \neq 0$, using a generator P and cyclic group G of a large prime order p.

— Then, it calculates the public key $T_{pub}$, where $T_{pub} = s \times P$. Where, s is a random master secret key (smc) and $s \in \mathbb{Z}_q^*$.

— The TA finally selects cryptographic hash functions $H_1, H_2, H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ and publishes its system parameters $H_1, H_2, H_3, p, q, P, G, E, T_{pub}$.

### 4.4.2 Vehicles' and RSUCs' registration

The vehicle sends a request to CA, and CA works as a registrar in our work. It gathers all relevant information about the vehicle and assigns a digital certificate to the vehicle. This certificate consists of a unique ID of the vehicle (the real identity obtained from the vehicle's motor manufacturer), the pseudonym ID (Pseudo), the private key, and the public key.

— The registration step starts with the vehicle $V_i$ submitting its real identity $ID_i$ via a secure channel to the TA. Then, TA will check if it is authentic.

— TA generates a corresponding $Pseudo_i$, $Pseudo_i = (Pseudo_{i1}, Pseudo_{i2})$ where : $Pseudo_{i1} = t_i \times P$ , $t_i \in \mathbb{Z}_q^*$, $L_i = t_i \times Tpub \oplus ID_i$ and $Pseudo_{i2} = ID_i \oplus H_1(sPseudo_{i1}, T_i)$.

— TA computes a hash function h where $h = H_1(ID_i \oplus Pseudo_i \oplus s)$ (after verification of the generation of pseudo-ID and the real identity ID of the vehicle.)

— TA stores together the hash function h, the pseudo-id ($Pseudo_i$) and the real identity $ID_i$ in its database.

— TA shares a randomly selected integer $\gamma_i$ with the vehicle $V_i$ and the $RSUC_i$ to calculate the partial private key $ppk_i$ of $V_i$, where $\gamma_i \in \mathbb{Z}_q^*$.

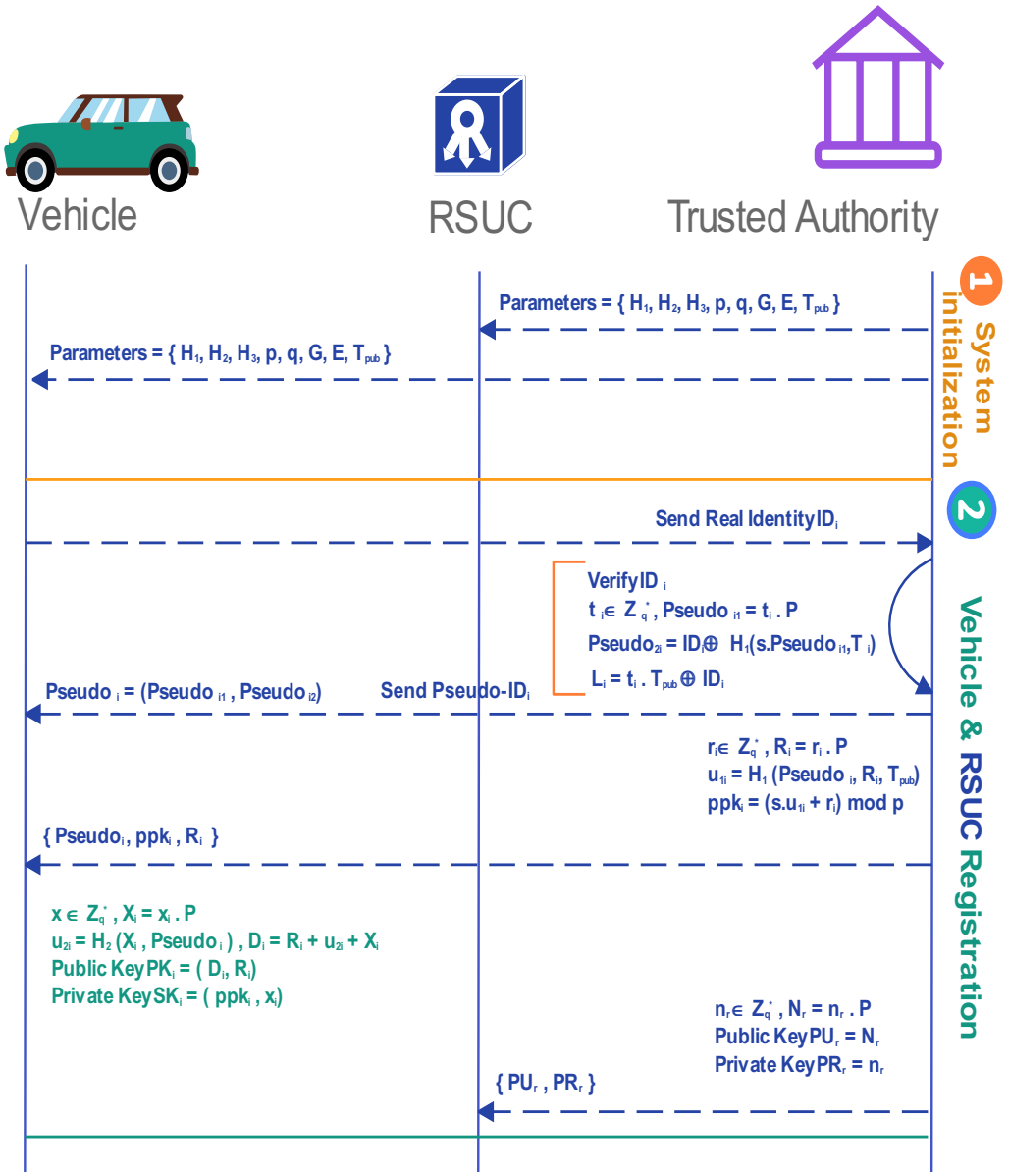



FIGURE 4.3 – System's initialization, vehicle, and RSUC registration, and exchanged messages diagram.

$R_i = r_i.P, u_{1i} = H_1(Pseudo_i, R_i, T_{pub})$ , $ppk_i = (r_i + s.u_{1i}) \mod p$.

— TA send $\{Pseudo_i, ppk_i, R_i\}$ to the vehicle $V_i$. Hence, the vehicle $V_i$ will saves it to its $RSUC_i$.

— The vehicle $V_i$ generates its public key (PK) and private key (SK) by taking a randomly selected secret integer $x_i$,, where $x_i \in \mathbb{Z}_q^*$ Then it calculates $X_i$ and $u_{2i}$, where $X_i = x_i.P$ and $u_{2i} = H_2(X_i, Pseudo_i)$. Therefore, the vehicle $V_i$ sets its keys (public and private) as below $PK_i = (D_i, R_i)$ and $SK_i = (ppk_i, x_i)$, where $D_i = R_i + u_{2i} + X_i$.

— The RSUCs are also registered by the TA. Each $RSUC_i$ has a public key $PU_i$ and private key $PR_i$. The TA takes a randomly selected number $n_j$, where $n_j \in \mathbb{Z}_q^*$ and sets it as its private key. Hence, $PR_j = n_j$ and computes its public key $PU_j = N_j$, where $N_j = n_j.P$

### 4.4.3 Vehicle authentication

In our system, we ensure that only legitimate vehicles can communicate with other entities in the network. Hence, each participating vehicle must be authenticated first by the TA when it tries to join the network. The authentication process is described as follows :

— The vehicle sends to the TA an authentication request containing the values of a timestamp T and the value of H $\{H, T_i\}$, where $H = h \oplus H_1(Pseudo_i \oplus R_i)$.

— The TA verifies the freshness of the authentication request by checking the timestamp. Then, it checks if the value of $h$ and $Pseudo_i$ are the corresponding credentials of the same vehicle registered in its database by checking the existence of H in the updated Blockchain.

Therefore, the TA verifies if the $h \oplus H_1(Pseudo_i \oplus R_i = H)$ is full-filled.

If the condition holds, the $RSUC_i$ takes a challenger which is a randomly selected integer $\alpha$, and encrypts it using the public key $PK_i$ of the vehicle $V_i$ as $ENC(\alpha, PK_i)$. Then, the $RSUC_i$ sends the result value to the vehicle $V_i$.

— Once the vehicle $V_i$ receives the encrypted value send by the $RSUC_i$, it decrypts it using its own secret private key $SK_i$ as $DEC(\alpha, SK_i)$ to generate another challenger $\omega$.

— Then, the vehicle $V_i$ will compute the hash value of both challengers $\alpha$ and $\omega$ as $HV = H_1(\alpha \oplus \omega)$.

— Next, the vehicle $V_i$ will encrypt a hash value HV using the public key $PU_i$ of the $RSUC_i$ as $ENC(HV, PU_i)$ and send a message to the $RSUC_i$, where the message contains $\{ENC(HV, PU_i), \omega\}$.

— Therefore, the $RSUC_i$ will decrypt the recevied message with its private key $PR_i$ as $DEC(HV, PR_i)$.

— Finally, the $RSUC_i$ will verify if $H_1(\alpha \oplus \omega) = HV$ holds.

— If the condition holds, then the authentication of the vehicle $V_i$ is successful and can communicate within the range of the $RSUC_i$. Otherwise, $V_i$ will be revoked from the network and the TA will add a revocation tag to the vehicle Pseudo-ID.

— Once the vehicle is authenticated successfully, the TA saves $H = h \oplus H_1(Pseudo_i \oplus R_i)$ into its memory pool.

— The saved term will be later mined and added as a new transaction to the Blockchain.

— Each time the vehicle changes its RSUC, it must register to the new RSUC with the same authentication process described in this subsection.

### 4.4.4 Message authentication

In order to provide integrity to our system, the messages (MSG) exchanged between vehicles and different nodes (other vehicles or RSUC) must be signed before sending using a private key. The receiver then will check it depending on the predefined equation. If the equation is held, the message will be accepted, else it will be rejected. We describe the message's authentication process as below :

— The vehicle $V_i$ takes a randomly selected integer $\beta$, where $\beta \in \mathbb{Z}_q^*$ to calculate its signature $\zeta_i$ as $\zeta_i = (F_i, K_i)$.
$F_i$ and $K_i$ are defined as below :
$F_i = \beta_i.P$ and $K_i = (\beta_i + u_{3i}(ppk_i + u_{2i}SK_i)) \mod p$, where $u_{3i} = H_3(Pseudo_i, ppk_i, MSG_i, F_i, T_i)$ and $u_{2i} = H_2(X_i, Pseudo_i)$.

— The vehicle $V_i$ send a message m to a nearby vehicle, where $m = \{ppk_i, Pseudo_i, MSG_i, \zeta_i, T_i\}$.

— Once the $RSUC_i$ receives the message m, it will verify the freshness first of all by checking the received timestamp value. If the condition is fulfilled. Then, it computes $u_{1i}$ as $u_{1i} = H_1(Pseudo_i, R_i, T_{pub})$ and calculates $u_{3i}$ as $u_{3i} = H_3(Pseudo_i, ppk_i, MSG_i, F_i, T_i)$.

— Finally, The $RSUC_i$ will check the condition $K_i.P = F_i + u_{3i}(Pseudo_i + u_{1i}.T_{pub})$. If, the condition holds, then the verifying entity will accept the received message by the vehicle. Else, the message

will be dropped.

## 4.5 Trust Model

In this section, we will detail the trust management process in our architecture. Trust management system enables vehicles to determine whether the received message is trustworthy. It allows the network administrators to revoke malicious vehicles.

### 4.5.1 Trust system's process

The trust management system within our architecture involves a multifaceted process designed to establish, monitor, and maintain trust within the connected vehicle network. Here's an overview of the key steps in the trust system's process :

#### 4.5.1.1 Rating generation and uploading

Rating generation refers to the process of evaluating and assigning trust ratings to individual vehicles or entities within the network. These ratings quantify the level of trust associated with each entity based on various factors and interactions. The key steps in rating generation include :

$$crd_i^k = l + e^{-\alpha.d_i^k} \tag{4.1}$$

where $crd_i^k$ is the message's credibility in group $G_k$ sent by vehicle i. $d_i^k$ is the distance between the location of the event and the message's sender. $\alpha$ and l are predefined parameters that contain the change rate of the message's credibility and the lower bound, respectively. Based on the Bayesian Inference, the aggregated credibility of a specific event e can be calculated by the receiver with the following equation :

$$P(e|CRD) = \frac{P(e).\prod_{i=1}^{N} P(crd_i|e)}{P(e).\prod_{i=1}^{N} P(crd_i|e) + P(\bar{e}).\prod_{i=1}^{N} P(crd_i|\bar{e})} \tag{4.2}$$

Where P($crd_i$|e)= $crd_i$ and $P(crd_i|\bar{e})$= 1 - $crd_i$.
P(e) is the probability of event e.
$P(e|CRD) \in$ [0,1].

— If $P(e|CRD)$ reaches a fixed threshold th+, the receiver considers this event as true and provokes positive ratings (+1) on messages correctly reporting this event.

— If $P(e|CRD)$ reaches a fixed threshold th-, the receiver considers this event as true and provokes negative ratings (-1) on messages inappropriately reporting this event.

— If $P(e|CRD)$ reaches or is equal to a fixed threshold th0, the receiver considers this event as a "draw" and provokes "draw" ratings (0) on messages suspiciously reporting this event. A deeper observation is required in this case. We allocate a time slot t, if the receiver does not change the rating value to a positive one, then draw ratings will be considered as negative ratings.

Rating value can be -1 for incredible messages, 0 for suspicious messages, and +1 for credible messages.

#### 4.5.1.2 Trust value offsets calculation

Trust value offsets calculation is a process within a trust management system that involves determining adjustments or offsets to an entity's trust value or rating based on specific criteria or events. These offsets are used to account for changes in trustworthiness or to respond to particular situations. We calculate the trust value offsets as follows :

$$OFF_i^k = \frac{(off_1.a) - (off_2 b)}{a + b} \tag{4.3}$$

where $off_i$ is the trust value offset of vehicle $i$ based on message k and $off_i \in$ [-1, 1]. a and b are the number of positive (+1) and negative (-1) ratings, whose weights are $off_1$ and $off_2$, respectively.

We then calculate $off_1$ and $off_2$ as bellow :

$$off_1 = \frac{S(a)}{S(a) + S(b)} \tag{4.4}$$

$$off_2 = \frac{S(b)}{S(a) + S(b)} \tag{4.5}$$

where $S()$ manipulates the sensitivity to the minority group of ratings.

#### 4.5.1.3 Mining and Consensus step

In our work, there is no central node. Hence, we have a decentralized architecture where no persistent entity manipulates the Blockchain. However, all the RSU Controllers (RSUCs) periodically elect one and only RSUC as the miner to manage the generation of new offset blocks. this chapter combines proof of stake and proof of work algorithms for the consensus mechanism. The stakes are the sum of calculated offsets in equation (3), and the resolve of the complex mathematical puzzle of the proof of work depends on these stakes. The nonce can only be found by the RSUC that has more stakes which will be elected as the miner to publish their blocks rapidly. Our method is calculated as below :

$$hash(Id_{RSUC}, t, prevHash, nonce) \leq TH_n. \tag{4.6}$$

Where $TH_n$ is the threshold hash value of $RSUC_n$ The nonce value is periodically changed by the RSUCs within the network, and the hash values are calculated. The election of the miner depends on the difficulty of having a nonce value satisfying the condition mentioned in equation (6). We define the current offset set of $RSUC_n$ as $OFFSET_n$. Therefore, we calculate the sum of absolute values of trust value offsets using the below equation :

$$H_n = min \left( \sum_{off_i^k \in OFFSET_n} |OFF_i^k|, H_{max} \right). \tag{4.7}$$

Therefore, the RSUC with a more significant $H_n$ is more conceivable to succeed in the election step and publish its block. This way, a considerable variation of trust values can be updated in the Blockchain. Hence, all segments in $OFFSET_n$ will be cleaned when the elected RSUC finally adds the offset block to the Blockchain.

### 4.5.2 Trust Process

In this section, we will provide a detailed description of the trust process within the connected vehicle network. This subsection focuses on the key components and steps involved in managing trust among network participants.

#### 4.5.2.1 Trust Request

The primary objective of this research is to enable vehicles within the network to ascertain the trust values of other vehicles by initiating a trust request directed at nearby Roadside Unit Controllers (RSUCs). The trust request is a structured communication that includes specific parameters, primarily consisting of the identity numbers of both the sender and the target vehicles. The trust request serves as a mechanism for vehicles to query the trustworthiness of their peers within the network. By providing the identity numbers of both the sender and the target vehicle, the trust request facilitates the retrieval of relevant trust values from the RSUCs. This information empowers vehicles to make informed decisions regarding their interactions and engagements with other network participants, ultimately enhancing the overall trust and security of the connected vehicle network.

Once the Roadside Unit Controller (RSUC) receives the trust request, it initiates a process to gather trust-related information concurrently. Here's how the process unfolds : (1) Request Verification : The RSUC begins by verifying the identity numbers provided in the trust request to ensure they are valid and correspond to actual vehicles within the network ; (2) Trust Value Retrieval : After verifying the identities, the RSUC accesses its database to obtain the current trust value of the target vehicle. This trust value may be based on historical behavior, interactions, and any recent trust offsets ; (3) Offset Collection : Concurrently, the RSUC collects trust value offsets associated with the target vehicle. These

offsets account for any recent events or trigger conditions that have affected the trustworthiness of the target vehicle ; (4) Offset Aggregation : The RSUC aggregates all collected trust value offsets, combining them with the current trust value of the target vehicle. This results in an updated trust value that reflects the current trustworthiness of the target vehicle, factoring in recent events or changes in behavior ; (5) Encryption : The aggregated trust value is then encrypted to ensure the security and privacy of the trust-related information during transmission ; (6) Transmission as Reply : Finally, the RSUC transmits the encrypted trust value as a reply to the sender's trust request. The sender, upon receiving this reply, can decrypt the information and use it to assess the trustworthiness of the target vehicle.

This process enables vehicles within the network to exchange trust-related information in a secure and privacy-preserving manner. It empowers network participants to make well-informed decisions based on the most up-to-date trust values and offsets, contributing to the overall trust and reliability of the connected vehicle network.

#### 4.5.2.2 Revocation Step

The revocation step is a critical component of a trust management system within a connected vehicle network. It involves the process of revoking or reducing the trust level of a vehicle or entity that has been identified as untrustworthy or engaged in malicious activities. Here's how the revocation step typically works :

— Detection of Misbehavior : The revocation process begins with the detection of misbehavior, which can include security breaches, non-compliance with network policies, or any other actions that compromise the trustworthiness of a vehicle or entity within the network.

— Identification of Untrustworthy Entity : The network's monitoring and assessment mechanisms identify the specific vehicle or entity responsible for the misbehavior. This identification is crucial for targeted revocation.

— Trust Level Adjustment : The trust management system initiates a trust level adjustment for the identified untrustworthy entity.

— Notification and Isolation : The affected entity is typically notified of the trust level adjustment or revocation. In the case of revocation, the entity may be isolated from certain network resources or interactions to prevent further harm.

— Feedback Mechanism : The trust management system may include a feedback mechanism that allows the affected entity to dispute the revocation or provide additional context. This feedback loop can help resolve disputes and refine the revocation process :

  * Periodic Reevaluation : Revoked entities are periodically reevaluated to determine if they have rectified their behavior or addressed the reasons for revocation. Trust may be reinstated based on improved behavior and compliance.

  * Audit Trail : Detailed records and logs are maintained throughout the revocation process, providing an audit trail of trust-related actions for accountability and transparency.

The revocation step is a crucial aspect of trust management, as it helps maintain the integrity and security of the connected vehicle network. It ensures that untrustworthy or malicious entities are appropriately addressed to protect the trustworthiness of the overall network and the safety of network participants.

## 4.6 Implementation

The implementation of our proposed framework was carried out using the Truffle framework [159], a versatile development toolkit for Ethereum-based smart contracts. To create a controlled and secure environment for development and testing, we employed Ganache [**?**], a local blockchain simulator that allowed us to iterate quickly and efficiently. During this phase, we meticulously crafted our smart contracts using Solidity [157], Ethereum's primary contract programming language, and harnessed Truffle's suite of tools for tasks such as compiling, migrating, and extensive testing of our contracts. Rigorous testing and

debugging were conducted on the local Ganache blockchain to ensure the correct and secure functionality of our smart contracts.

Upon reaching a satisfactory level of confidence in our contracts' local operation, we proceeded to deploy them to the Ethereum testnet [**?**], a real blockchain environment that mirrors the Ethereum network's features. This step marked the transition from development to more advanced testing and integration, enabling us to validate the contracts' performance and functionality in a real-world blockchain setting. Alongside this, we engaged in thorough performance and security audits to identify and rectify any vulnerabilities or inefficiencies within our smart contracts. In our experiments, we utilized a gas price of $1Gwei$, where $1Gwei = 10^9 wei = 10^{-9}$ ether. To provide context for the cost in a more widely recognized currency, 1 ether was equivalent to $1,629USD$. Table 1 presents a comprehensive analysis of the cost and security aspects of our smart contract-based framework. Notably, our cost analysis reveals that all smart contract deployments are characterized by low costs. This cost-effectiveness is a significant achievement, as it ensures that our framework is economically accessible and sustainable for users and stakeholders. The low-cost nature of our smart contract deployments reflects our commitment to efficiency and affordability within the blockchain ecosystem. It signifies that users can engage with our framework without incurring substantial expenses, enhancing the accessibility and attractiveness of our platform. This cost-efficient approach aligns with our broader goal of providing a blockchain-based solution that is not only secure but also practical and economically viable for a wide range of use cases. Users can leverage the benefits of blockchain technology without being deterred by high deployment costs, making our framework a compelling choice in the blockchain landscape.

TABLE 4.1 – Cost and Security analysis of our smart contract-based framework

| **Parameters** | **MSC** | **TSC** | **RSC** | **ACSC** |
|---|---|---|---|---|
| Gas Used | 3528732 | 326822 | 1372568 | 876436 |
| Costs (Ether) | 0.003528732 | 0.000326822 | 0.001372568 | 0.00087 |
| Costs (USD) | 5.6 | 0.150 | 2.19 | 1.39 |
| EVM Code Coverage | 87.5 | 86 | 72 | 15.6 |
| Integer Underflow | False | False | False | False |
| Parity Multisig Bug 2 | False | False | False | False |
| Callstack Depth Attack Vulnerability | False | False | False | False |
| Transaction-Ordering Dependence (TOD) | False | False | False | False |
| Timestamp Dependency | False | False | False | False |
| Re-Entrancy Vulnerability | False | False | False | False |

## 4.7 Security analysis

The security of our blockchain-based framework was rigorously assessed for vulnerabilities using the Oyente [155] analyzer. Oyente is a well-known security analysis tool specifically designed for Ethereum smart contracts, providing comprehensive coverage for potential vulnerabilities and weaknesses within the code. Through this analysis, we aimed to identify and address any security-related issues that could pose risks to the integrity and reliability of our smart contracts. By leveraging Oyente, we conducted a thorough examination of our smart contracts' codebase, scrutinizing them for common security pitfalls such as reentrancy vulnerabilities, integer overflow/underflow issues, and unauthorized access concerns (see Table. 4.1). This includes :

— Integer Underflow : Integer underflow occurs when a variable of a fixed size (e.g., 256 bits in Ethereum) exceeds its maximum value, causing it to wrap around to the minimum value. This can lead

to unexpected and potentially malicious behavior. Our smart contracts are rigorously designed and thoroughly tested to prevent integer underflow vulnerabilities. We use safe arithmetic operations and checks to ensure that all integer values stay within expected bounds, eliminating the risk of underflow-related issues.

— Parity Multisig Bug : The Parity Multisig Bug refers to a critical vulnerability in the Parity wallet that allowed an attacker to exploit a flaw in the smart contract code, resulting in the loss of a significant amount of ether. Our smart contracts are not susceptible to this specific bug because we have followed best practices in smart contract development, conducted extensive testing, and learned from past vulnerabilities to ensure the security of our code.

— Transaction-ordering dependence (TOD) : Transaction-ordering dependence, also known as "front-running," occurs when an attacker observes pending transactions and intentionally reorders them to their advantage. We have implemented safeguards in our smart contracts to minimize the impact of TOD. Our contracts are designed to handle transactions securely and consistently, regardless of the order in which they are processed by the blockchain.

— Timestamp Dependency : Timestamp dependency vulnerabilities arise when smart contracts rely on the block timestamp to make decisions. Attackers can manipulate timestamps to their advantage. In our smart contract design, we have minimized timestamp dependency by using block numbers and other blockchain-related data that are less susceptible to manipulation, ensuring that our contracts operate securely even in the presence of timestamp-related risks.

— Re-Entrancy Vulnerability : Re-entrancy vulnerabilities occur when a malicious contract can repeatedly call back into another contract before the first call completes. This can lead to unexpected or unauthorized behavior. Our smart contracts are constructed with meticulous care to eliminate re-entrancy vulnerabilities.

The proposed Blockchain-based trust management framework ensures Authentication, Traceability, Integrity, and Resistance to DDoS attacks through a combination of cryptographic techniques, smart contract functionalities, and decentralized architecture :

(1) Authentication : The Management Smart Contract (MSC) plays a central role in authenticating vehicles during the registration process. It verifies the authenticity of vehicle identities and ensures compliance with network regulations. Only legitimate vehicles are registered, preventing unauthorized entities from participating in the network.

(2) Traceability : The use of blockchain technology ensures that all transactions and trust-related decisions are recorded as immutable records on the blockchain. This creates a transparent and auditable trail of actions, enhancing traceability. The Trust Smart Contract (TSC) records trust scores on-chain, providing a clear history of trustworthiness.

(3) Integrity : Data integrity is maintained through cryptographic techniques, ensuring that data within the blockchain remains tamper-proof. Smart contracts and trust scores recorded on the blockchain are protected from unauthorized modifications. Access Control : The Access Control Smart Contract (ACSC) enforces granular access controls, preventing unauthorized access attempts. This enhances the overall integrity of the system by limiting access to authorized entities only ; and (4) Resistance to DDoS Attacks : The decentralized architecture of the blockchain network enhances resistance to DDoS attacks. With multiple nodes participating in consensus, it becomes challenging for attackers to overwhelm the network by flooding it with traffic.

By combining these elements, the proposed framework ensures robust authentication, traceability, data integrity, and resistance to DDoS attacks, making it a secure and reliable solution for trust management within Intelligent Transportation Systems (ITS).

## 4.8 Conclusion

This chapter presents a pioneering framework built upon Blockchain technology, employing multiple smart contracts to instill trust and guarantee security in prospective Software-Defined Vehicular Net-

works (SDVN). Our approach is entirely distributed, transparent, secure, tamper-proof, and reliable. The experimental results underscore the superior performance of our proposed system, particularly in terms of adaptability, security, efficiency, and cost-effectiveness. These attributes position our solution as a highly promising candidate for advancing the development of decentralized trust management systems within the domain of Intelligent Transportation Systems (ITS).

CHAPITRE 5

# Federated Learning-based Intrusion Detection System for Connected Vehicles

## Table des matières


5.1 Introduction . . . 86
5.2 Related Work and Background . . . 86
5.2.1 Blockchain-based IDS . . . 87
5.2.2 Machine and Deep Learning IDS . . . 87
5.3 System Overview . . . 88
5.4 System Model . . . 88
5.4.1 Network components . . . 88
5.4.2 Powers of Smart Contracts . . . 91
5.4.3 Adversary Model . . . 92
5.5 Proposed VFed-IDS Architecture . . . 92
5.5.1 Classification Step . . . 92
5.5.2 Malicious vehicles detection . . . 93
5.6 Simulations . . . 93
5.6.1 Experimental setup . . . 93
5.6.2 Description of NSL-KDD dataset . . . 95
5.6.3 Attacks types . . . 97
5.7 Results' Discussion . . . 99
5.7.1 Impact of rounds number on model's metrics . . . 99
5.7.2 ROC Curve . . . 112
5.8 Open issue . . . 116
5.8.1 Federated Learning Clients' Selection . . . 116
5.8.2 Rounds' total number of FL process . . . 117
5.9 Conclusion . . . 117

## 5.1 Introduction

Recently, cyber-threats have grown because of vulnerabilities in some internet-connected devices, especially the Connected Vehicles (CV) [163], which frequently make them easy targets. DDoS attacks, particularly, are highly challenging to detect compared to other attacks because of their capacity to hide themselves as honest traffic in the network. DDoS attacks are exponentially increasing daily in Connected Vehicles due to the extensive usage of intelligent wireless interface software [164], such as IoT, V2X, and 5G/6G, used for communication and sensing. This leads to the intensive development of new IDS to confront cyber risks.
The utilization of ML methods in the field of cyber-security, as discussed in [162], has garnered significant interest due to their capacity to enhance decision-making and enable efficient automated operations. ML techniques have found successful applications across diverse cyber-security domains, such as spam detection, malware identification, user authentication, software vulnerability detection, and DDoS attack detection. These methods have shown great promise by delivering high accuracy and recall rates while keeping false positives at a minimum.
The demand for vehicular networks's safety and infotainment services (e.g., accident avoidance, driver assistance, video on demand, and infotainment applications) is increasing. Vehicles nowadays can support various entertainment and comfort applications, but emerging these services opens up additional challenges regarding Quality of Service (QoS), privacy, and security. Integrating novel technologies, such as IoT, Edge Computing, Fog computing, Cloud Computing, and Artificial Intelligence, represents one of the major research topics in vehicular networks. Researchers are paying significant attention to deploying AI techniques, such as ML and Deep Learning (DL), in many application domains, not only in robotic, data analytic, or healthcare domains but also in vehicular networks, to solve the above-mentioned challenging concerns. Moreover, providing node safety and reducing data latency and accident rate are some of the most significant goals in vehicular networks.
Since unstable network leads to routing issues, integrating ML techniques (e.g., Support Vector Machine (SVM), k-nearest neighbors (k-NN), k-mean clustering, Naive Bayes (NB), Conventional Neural Network(CNN), etc..) in vehicular networks with further data analytic will improve its stability in term of safety (e.g., vehicle safety, collision alert, etc..), traffic management (e.g., traffic scheduling, traffic congestion, traffic monitoring, etc..) and in terms of communication (e.g., link management, data congestion control, routing and misbehavior detection, etc..).
The key contributions of this chapter can be summarized as follows :

— We propose the VFed-IDS : a decentralized, trustworthy, flexible and scalable IDS for connected vehicles based on Blockchain and Federated Learning.

— VFed-IDS is composed of three main layer : Central layer, local layer and Blockchain layer. The central layer for training/aggregating the global models, the local layer for training local models and the Blockchain is for calculating the hash values of local models and to manage the list of collaborating vehicles in the FL process. Hence, this only enable authenticated vehicles to collaborate.

— Our architecture enhances considerably the autonomous behaviour of vehicles in making independent decisions about cyber threats.

— We develop our smart contract VFed-SC to manage the list of participating vehicles into the FL process. The VFed-SC is developed under the Ethereum Blockchain smart contract.

— We tested our proposed work with the well known NSL-KDD dataset.

— We evaluate the VFed-IDS in terms of a set of criteria : Precision, Recall, Accuracy, F-measure and False Positive Rate.

— Our architecture shows that it enhances the privacy in IoV, provides a high accuracy rate up to 99% and it copes with large scale networks.

## 5.2 Related Work and Background

In this section, we discuss and analyse some of the critical-related works found in the literature. Firstly, we introduce the research work on intrusion detection systems in IoV based on Federated Learning and Blockchain. Then, we summarize these works in table 5.1 based on : integration of Blockchain, integration

of Smart contract, integration of FL, does the work present an IDS ?, does this work cope with the IoV ?

### 5.2.1 Blockchain-based IDS

In this subsection, we discuss the Blockchain-based IDS. [168] designed a trustworthy distributed blockchain-based platform for vehicular systems. In this work, the exchanged messages from nearby vehicles are validated depending on a Bayesian inference model. Then, the vehicles generate ratings according to the validation results. In this work, the RSUs estimate the trust value offsets of participating nodes and store them in blocks. This solution improves its performance in terms of privacy and security in the network. However, more significant attention to the cost and execution time must be considered.

[169] integrated Blockchain technology in their work to create a trustworthy platform for vehicles to identify malicious nodes. In this solution, the vehicles participate in making decisions about other nodes in the network by validating packets only from authenticated nodes. The vehicles in this work also participate in creating and sharing new blocks in the Blockchain.

Another Blockchain-based work was introduced by [170]. The authors in this work integrated Blockchain technology to improve the vehicles' and exchanged data authentication. This work presented a defensive mechanism to identify malicious vehicles with manipulated data.

[171] integrated Blockchain technology to develop an authentication mechanism. This work aims to enhance the privacy of the network. Hence, the exchanged messages must be authenticated, too, using asymmetric keys and the PoW and PBWT algorithms.

### 5.2.2 Machine and Deep Learning IDS

[172] proposed a robust and low-cost IDS against DDoS attacks in IoT. This solution depends on the collaborative and distributed training model paradigm. In this solution, the authors positioned the training model at the edge server to cope with the limited resources of IoT devices.

[173] presented a Fed-TH architecture based on a novel federated deep learning. This work integrates a container-based edge-computing framework with the FL to establish a robust and reliable intrusion detection system for cyber threats in industrial information physical systems.

Another FL-based work was introduced by [174]. The authors in this work designed a platform called FedIoT, which depends on the algorithm FedDetect to identify a more extensive scope of attacks calsses that may appear on multiple IoT devices in a Raspberry Pi-based environment.

As artificial intelligence technology rapidly advances and intelligent applications gain popularity, the proliferation of vast amounts of Internet of Things (IoT) data has become commonplace. This surge in data generation has heightened consumer expectations regarding the protection of their data privacy. Traditional IoT network security detection methods, heavily reliant on centralized machine learning and deep learning, need reevaluation to meet the contemporary demands of securing IoT networks. In response to the evolving requirements of IoT cybersecurity, researchers are exploring innovative approaches that integrate federated learning and edge computing paradigms.

Several researchers, including Ghimire and Rawat in 2022 and Khan et al. (citation pending), have proposed novel IoT intrusion detection methods based on collaborative training. In 2019, Nguyen et al. introduced Doot, a federated learning-based intrusion detection framework designed for identifying specific device types in home automation settings. Similarly, Mothukuri et al. (2021) proposed a federated learning-based anomaly detection system to improve the accuracy of identifying and classifying attacks in IoT networks, employing a combination of Gated Recurrent Units (GRUs) layers and ensembles.

Taking a unique approach, Li et al. (2021b) combined federated learning and edge computing to establish an efficient and cost-effective defense mechanism against Distributed Denial of Service (DDoS) attacks in the Industrial Internet of Things (IIoT). This strategy mitigates the limitations posed by the limited resources of IoT devices by shifting model training to edge servers. Meanwhile, Zhang et al. (2022) introduced a framework for preserving the integrity of IoT devices by detecting cyberattacks.

In a different context, Li et al. (2021a) proposed a federated learning-based intrusion detection approach for Industrial Cyber-Physical Systems (CPSs). This approach involves collaborative training among various security agents employing deep learning models, creating an efficient and flexible cyber threat detection system within industrial information and physical systems. While these research efforts explore the benefits of network security detection methods based on federated learning from various perspectives, it's essential to note that they often do not fully address the security issues associated with intrusion detection methods based on federated learning.

Table 5.1 – Related works.

| Paper | Blockchain | Smart Contract | Fed. Learning | IDS | IoV |
|---|---|---|---|---|---|
| [168] | Yes | No | No | No | Yes |
| [169] | Yes | No | No | Yes | Yes |
| [170] | Yes | No | No | Yes | Yes |
| [171] | Yes | No | No | No | Yes |
| [6] | Yes | No | No | Yes | No |
| [172] | No | No | Yes | Yes | No |
| [173] | No | No | Yes | Yes | No |
| [174] | No | No | Yes | Yes | No |
| **Our work** | **Yes** | **Yes** | **Yes** | **Yes** | **Yes** |

## 5.3 System Overview

In this section, we will describe the privacy-preserving process between multiple vehicles, participating as edge servers, and the SDNCs as the central servers. We represent the proposed architecture in Figure 5.1. Our architecture permits numerous vehicles and SDNCs to participate in the privacy-preserving operation by combining the potentials of the Blockchain and an advanced Deep Learning technique, Federated Learning, using a smart contract to manage the process. Our smart contract will first be created in the Blockchain by the central server SDNC. Then, the participating and honest vehicles will only be added as collaborating servers. Consequently, our architecture provides the reliability and integrity of the system due to the integration of the Blockchain. In this system, the privacy-preserving process starts with initializing a global model and then broadcasting it to the vehicles in the local layer. Moreover, the collaborating vehicles will train their local models with their private datasets and calculate their hash values, which stops any entity from rebuilding a collaborator's private data from its model updates. Therefore, they will upload their trained models' updates and try to add the hash values to the Blockchain. Finally, the SDNC will verify the uploaded models' updates and aggregate it in the global model.

## 5.4 System Model

This section introduces our IDS based on Federated Learning and Blockchain, as illustrated in figure 5.1. This IDS comprises SDNC, the central server, RSUs, the local intrusion detection servers, and multiple connected vehicles. This work will lead the way for vehicles to participate in the training process of local models. The list of symbols used to describe our architecture is listed in table 5.2.

### 5.4.1 Network components

#### 5.4.1.1 Central Layer

The central layer is composed by the SDNCs. This layer is responsible of the global model's initialization. The SDNC will send the global model to the local layer's servers (the vehicles). It also aggregates the uploaded local models trained by the vehicles to participate in assembling the model. Finally, the major function of this layer is to detect the malicious entities in the network. The new global model aggregated by the SDNC is set after receiving the local model from each vehicle $V_j$ designated as follows :

$$gm^{r+1} = \frac{nbr_j}{NBR}.\sum_{j=1}^{N}.lm^{t}_{j,r+1} \tag{5.1}$$

Table 5.2 – Used symbols

| Symbol | Description |
|---|---|
| N | Total number of vehicles |
| j | The vehicle j |
| r | round r of the FL process |
| t | Phase t of round r of the FL process |
| $lm_{j,r}$ | Local model of vehicle j at round r |
| $lm^{t}_{j,r}$ | Local model of vehicle j at phase t of round r |
| $gm_j$ | Global model of vehicle j |
| $gm^0$ | Initial Global model |
| V | Set of vehicles |
| $DS_j$ | Private data set of vehicle j |
| $\zeta$ | Learning rate |
| S | Size of the data set |
| $\nabla.f()$ | The objective function |
| $I_{j,n}$ | Input of the objective function |
| $O_{j,n}$ | Output of the objective function |
| $nbr_j$ | The number of trained data sample of $DS_j$ |
| $NBR$ | The sum of trained data sample of datasets |
| $VFed-SC$ | Smart Contract based on FL for vehicular networks |

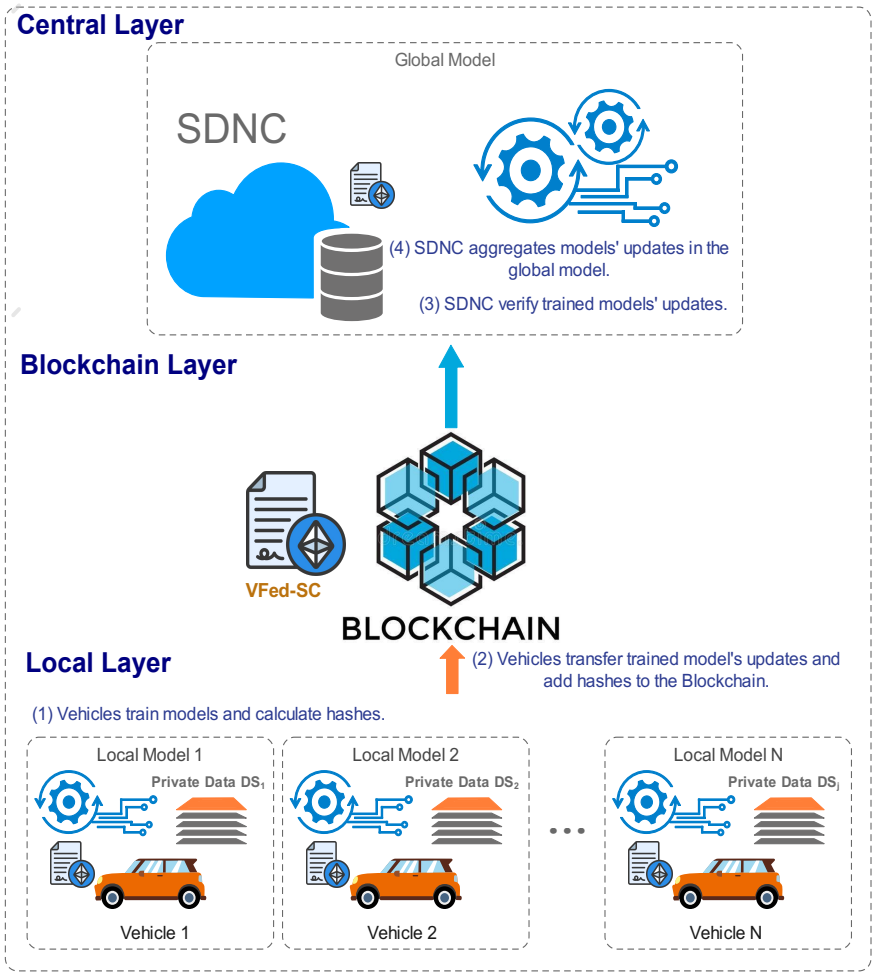



FIGURE 5.1 – Federated Learning and Blockchain based IDS for Connected Vehicles

Where : $NBR = \sum_{j=1}^{N} nbr_j$ and $nbr_j$ represents the number of trained data sample of dataset $DS_j$.

#### 5.4.1.2 Local Layer

This layer is composed of participating connected vehicles. Each vehicle will utilize its private dataset to train its local IDS model in this work. All private datasets combine both normal and anomalous traffic. We assume that we have N vehicles, which signifies N edge nodes in the Edge layer designated by :
$V = \{V_1, V_2, ...V_N\}$.
Private datasets are represented by :
$DS_j = \{DS_1, DS_2, ...DS_N\}$.
The FL process is established during multiple iterations, where each vehicle will utilize a stochastic gradient descent (SGD) algorithm to train its private model $m_j$ with its local data set $DS_j$ The local training process is denoted by the following formula :

$$lm^t_{j,r+1} = lm^{t-1}_{j,r+1} - \frac{\zeta^t_{j,r+1}}{S^t_{j,r+1}} . \sum_{n \in DS^t_{j,r+1}} . \nabla f(lm^{t-1}_{j,r+1}, A_{n,j}, Z_{n,j}). \tag{5.2}$$

Where :
$lm^t_{j,r+1}$ is the local model of $V_j$ at phase $t$ of round $r+1$.
The learning rate here is denoted by $\zeta$.
$DS^t_{j,r+1}$ is randomly selected from the local dataset $DS_j$ of $V_j$.
$S^t_{j,r+1}$ represents the size.
$A_{n,j}$ and $Z_{n,j}$ represent the input and output vectors of data sample $n$ in $DS_j$.
And $\nabla.f()$ is the local objective function.

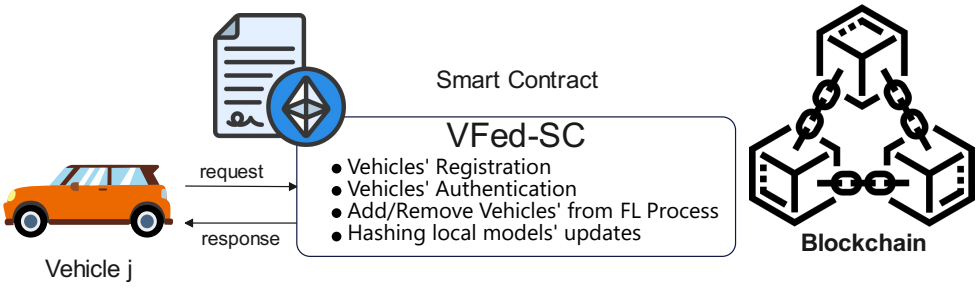



FIGURE 5.2 – Our smart contract VFed-SC process.

#### 5.4.1.3 Blockchain Layer

In this work, the Blockchain layer, where we deploy our smart contract, manipulates the collaborative privacy-preserving learning operation across multiple vehicles. First, the SDNC will create and deploy the smart contract VFed-SC in Ethereum Blockchain. Then, it will manage the collaborating vehicles through it. At this step, the SDNC will manage the subscription of the collaborators by permitting or withdrawing the vehicles to participate in the privacy-preserving learning operation in a decentralized manner, which improves the flexibility and trustworthiness of the system. The deployed smart contract will hash the trained local models' updates before sending them to the SDNC using the SHA-256 hashing function.

#### 5.4.1.4 Characteristics of Smart Contract VFed-SC

We illustrate the main characteristics of the smart contracts as follows :

— **Distributed** : Every participating node ensures they possess a copy of the smart contract conditions, and it remains impervious to modifications by any single entity. This smart contract is replicated and distributed across all network entities, encompassing both central and local layers.
— **Deterministic :** The VFed-SC exclusively carries out its designated functions when the stipulated prerequisites are met. The ultimate impact of the smart contract on the system remains unaltered, irrespective of the entity executing it.
— **Autonomous :** There are no third parties involved. The smart contract is shared between the involved parties upon its creation. There are no intermediaries, reducing the potential for coercion and empowering the parties involved. Additionally, the smart contract is upheld and executed by all nodes on the network, effectively relinquishing centralized control from any single entity.
— **Firm :**The VFed-SC is immutable in the sense that once it is deployed and activated, it cannot be altered. However, it can be terminated or removed.
— **Customizable :** Usually, it can be tailored or customized before deployment to fulfill the user's specific requirements.
— **Transparent :** The smart contract is consistently stored on a publicly distributed Blockchain, making its code accessible to everyone, regardless of their participation in the smart contract.
— **Trustless :** There is no need for third parties to demonstrate the integrity of the process or to verify whether the required conditions are met.
— **Self-verifying :** It is self-verifying due to automated capabilities.
— **Self-enforcing :** The VFed-SC is self-enforcing when the conditions and rules are met at all stages.

### 5.4.2 Powers of Smart Contracts

We describe in this subsection the powers of smart contracts as follows :

— **Accuracy :** The accuracy of smart contracts is limited to how precisely a programmer has coded them for execution.
— **Automation :** Smart contracts can automate tasks and processes that are typically done manually.
— **Speed :** They use software code to automate tasks, reducing the time required for processes that involve human interaction. Since everything is coded, the time taken to complete tasks with a smart contract is determined by the execution of the code itself.
— **Backup :** Each node in the blockchain maintains a copy of the shared ledger, offering a robust backup system.

— **Security :** The use of cryptography ensures the security of transactions. Even if someone manages to crack the encryption, the hacker would need to modify all the blocks that come after the block that has been tampered with. It's important to note that this is a difficult and computation-intensive task, making it practically impossible for a small or medium-sized organization to achieve.
— **Manages information :** Smart contracts are responsible for managing user agreements and storing information related to applications, such as domain registration, membership records, and more.
— **Multi-signature accounts :** Smart contracts offer support for multi-signature accounts, enabling the broadcast of transactions to other accounts once all involved parties reach an agreement.

### 5.4.3 Adversary Model

Researchers face a significant challenge in enhancing the trustworthiness of participants within the Federated Learning (FL) framework, primarily to meet security requirements.

When training intrusion detection models for connected vehicles using FL, a threat arises from malicious collaborating vehicles situated in the local layer (edge servers) under the control of attackers. These adversaries may launch DDoS attacks, thereby impacting the availability of the model. The primary goal of this adversary model is to compromise the cybersecurity of the IoV by manipulating the global model trained in the FL process. Consequently, malicious traffic data could be misclassified as legitimate. As a result, the malicious entities behind these attacks may be falsely identified as legitimate nodes and allowed to participate and collaborate within the FL process.

In the context of these attacks, the adversary entity, denoted as 'z,' has limitations. It can only manipulate its private local data represented as $DS_z$ to create a falsified local training model. However, it does not possess the capability to manipulate the local models of other entities.

## 5.5 Proposed VFed-IDS Architecture

The primary objective of our work is to develop an efficient IDS for connected vehicles based on FL and Blockchain using the VFed-SC smart contract. This latter is installed in the SDNC in the central layer. Hence, the malicious locally trained models by attacking vehicles will be detected before being uploaded to the global model.

### 5.5.1 Classification Step

In the VFed-IDS, participating vehicles employ their private dataset to train their local models in the local layer after receiving the initial global model from the SDNC. Once these local models are conducted, the vehicles encrypt them by calculating their hash values, which will be uploaded and added to the Blockchain and then to the central server, the SDNC, which aggregates them after verification. At this phase, the SDNC gathers the obtained loss in the local layer, the data from the samples concerned in the training, and the vehicles' local models.
The inconsistency between prediction and actual values represents the estimated loss of the training model. The loss is a non-negative value, which qualifies the robustness of the model. The most robust models have the smallest loss values. In the case of multi-classification situations, the loss function is computed with the following equation :

$$H = -\sum_{j=0}^{c} X_j . \log \hat{X}_j \tag{5.3}$$

Where : $\hat{X}_j$ is the prediction model result, $X_j$ is the true label and c denotes the category.
In VFed-IDS, we study a binary classification intrusion detection model, where c can have the value of 0 or 1.
To assess the participating vehicles in our system, we calculate its scoring function value based on its loss function and its model's sample size. The scores are calculated depending on the following equation :

$$SCORE_j^r = \frac{n_j}{NBR} . \frac{1}{H_j^r} \sum_{j=1}^{N} . \frac{1}{H_j^r} \tag{5.4}$$

where : $H_j^r$ is the loss obtained from training local model j of the vehicle j at round r.

### 5.5.2 Malicious vehicles detection

We describe, in this section, the process of detecting malicious vehicles in the network. In our architecture, we have distributed data. Hence, the obtained trained local models of participating vehicles in the local layer have similarities. Malicious vehicles are identified based on their Manhattan similarity values with other participators, and their score values calculated with equation 4.
The similarities are calculated with the following equation :

$$Sim = \sum_{j=1, j\neq i}^{N} |Sim_j - Sim_i| \tag{5.5}$$

**Algorithm 2:** Malicious Vehicle's Detection Algorithm

**Data:** Vehicle $V_j$, private dataset $DS_j$, $N$ number of vehicles and their private dataset DS
**Result:** Malicious Vehicles' Detection
Initialize the global model $gm^0$;
Distribute the global model $gm^0$ to the participating Vehicles;
**At the local training, at round** $r$;
**for** *j in N* **do**
    Train the local model $lm_{j,r}$ based on its private dataset $DS_j$ and global model $gm^r$;
    Calculates the hash value of $lm_{j,r}$;
    Adds the hash value of $lm_{j,r}$ to the Blockchain;
    Uploads $H_j^r$ and $NBR_j$ to the SDNC ;
**At the global training, at round** $r$;
**for** *j in N* **do**
    Calculating $SCORE_j$ of Vehicle $j$ according to $H(j)$;
    Similarity Calculation $Sim(j)$;
**Malicious Vehicle Detection**;

## 5.6 Simulations

In this section, we detail the experimental setup, description of NSL-KDD dataset and its attacks types, and evaluation of the robustness of the trust model metrics and then present the experimental results and analyze them as shown below. In each scenario, we divide the NSL-KDD dataset between the participating connected vehicles (clients). Hence, each vehicle will have its own private dataset, which contains a portion of the different cyber threats presented in the main dataset. We run our experiments on Google Colaboratory [175]. In each scenario, the parameters of the global model are initialized randomly.

### 5.6.1 Experimental setup

The environment setup and different conducted scenarios are given in Table 5.4.

Table 5.3 – List of Features in NSL-KDD Dataset

| No. | Feature | Description |
|---|---|---|
| 1 | duration | Length of time a connection has been active. |
| 2 | protocol_type | Type of network protocol used for the connection (e.g., TCP, UDP, ICMP). |
| 3 | service | Network service on which the connection was requested (e.g., http, ftp, smtp). |
| 4 | flag | Status of the connection (e.g., S0, S1, S2, REJ). |
| 5 | src_bytes | Number of data bytes sent by the source. |
| 6 | dst_bytes | Number of data bytes received by the destination. |
| 7 | land | Indicates whether the connection is from/to the same host and port. |
| 8 | wrong_fragment | Number of "wrong" fragments. |
| 9 | urgent | Number of urgent packets. |
| 10 | hot | Number of "hot" indicators. |
| 11 | num_failed_logins | Number of failed login attempts. |
| 12 | logged_in | Indicates whether a user is logged in. |
| 13 | num_compromised | Number of compromised conditions. |
| 14 | root_shell | Indicates whether a root shell is obtained. |
| 15 | su_attempted | Indicates whether a "su root" command was attempted. |
| 16 | num_root | Number of "root" accesses. |
| 17 | num_file_creations | Number of file creation operations. |
| 18 | num_shells | Number of shell prompts. |
| 19 | num_access_files | Number of operations on access control files. |
| 20 | num_outbound_cmds | Number of outbound commands in an FTP session. |
| 21 | is_hot_login | Indicates whether the login belongs to the "hot" list. |
| 22 | is_guest_login | Indicates whether the login is a "guest" login. |
| 23 | count | Number of connections to the same host as the current connection in the last 2 seconds. |
| 24 | srv_count | Connections' number to the same service as the current connection in the last 2 seconds. |
| 25 | serror_rate | Percentage of connections that have "SYN" errors. |
| 26 | srv_serror_rate | Percentage of connections that have "SYN" errors to the same service. |
| 27 | rerror_rate | Percentage of connections that have "REJ" errors. |
| 28 | srv_rerror_rate | Percentage of connections that have "REJ" errors to the same service. |
| 29 | same_srv_rate | Percentage of connections to the same service. |
| 30 | diff_srv_rate | Percentage of connections to different services. |
| 31 | srv_diff_host_rate | Percentage of connections to different hosts. |
| 32 | dst_host_count | Number of connections to the same destination host as the current connection in the last 2 seconds. |
| 33 | dst_host_srv_count | Number of connections to the same destination service as the current connection in the last 2 seconds. |
| 34 | dst_host_same_srv_rate | Percentage of connections to the same service on the destination host. |
| 35 | dst_host_diff_srv_rate | Percentage of connections to different services on the destination host. |
| 36 | dst_host_same_src_port_rate | Percentage of connections to the same source port on the destination host. |
| 37 | dst_host_srv_diff_host_rate | Percentage of connections to different hosts on the destination service. |
| 38 | dst_host_serror_rate | Percentage of connections that have "SYN" errors to the destination host. |
| 39 | dst_host_srv_serror_rate | Percentage of connections that have "SYN" errors to the destination service. |
| 40 | dst_host_rerror_rate | Percentage of connections that have "REJ" errors to the destination host. |
| 41 | dst_host_srv_rerror_rate | Percentage of connections that have "REJ" errors to the destination service. |

Table 5.5 – Existing samples in NSL-KDD dataset.

| **Attack Class** | **Records** |
|---|---|
| Normal | 77232 |
| DoS | 53387 |
| Probe | 14077 |
| R2L | 3702 |
| U2R | 119 |

Table 5.4 – Scenarios details.

| Scenario | Clients | Rounds | Epoch | With MLP Executed in | With RNN Executed in |
|---|---|---|---|---|---|
| Sc1 | 10 | 5 | 1 | 36s 323 ms | - |
| Sc2 | 10 | 5 | 5 | 57 s 347 ms | - |
| Sc3 | 10 | 10 | 1 | 1m 26 s 47 ms | - |
| Sc4 | 10 | 10 | 5 | 2m 52 s 381 ms | 36min 25s |
| Sc5 | 10 | 25/30 | 5 | 6m 44s 38ms | 47min 58s |
| Sc6 | 10 | 50 | 5 | 9m 53s 5ms | - |
| Sc7 | 25 | 5 | 5 | 4m 13s 184ms | - |
| Sc8 | 25 | 10 | 5 | 4m 44s 892ms | - |
| Sc9 | 25 | 25/30 | 5 | 14m 52s 330ms | - |
| Sc10 | 25 | 50 | 5 | 27m 26s | - |
| Sc11 | 50 | 25/30 | 10 | 37m 24s 378ms | - |
| Sc12 | 50 | 50 | 10 | 41m 39s 112ms | - |
| Sc13 | 100 | 25 | 10 | 3h 13m | - |
| Sc14 | 100 | 50 | 11 | 2h 44m 2s | - |

In each scenario, we divide the NSL-KDD dataset between the participating connected vehicles (clients). Hence, each vehicle will have its own private dataset, which contains a portion of the different cyber threats presented in the main dataset. In each scenario, the parameters of the global model are initialized randomly.

### 5.6.2 Description of NSL-KDD dataset

The NSL-KDD dataset, short for the "NSL-KDD Intrusion Detection Dataset", is a well-known benchmark dataset widely used for evaluating and developing Intrusion Detection Systems (IDS) and network security solutions [176]. It was created as an improvement over the original KDD Cup 1999 dataset to address some of its limitations and challenges. The NSL-KDD dataset is specifically designed to support

Table 5.6 – NSL-KDD Train and NSL-KDD Test dataset details.

| **Class** | **Total** | **Normal** | **DoS** | **Probe** | **R2L** | **U2R** |
|---|---|---|---|---|---|---|
| **NSL-KDD Train** | 125973 | 77232 | 53387 | 14077 | 3702 | 119 |
| **NSL-KDD Test** | 22544 | 13823 | 9555 | 2520 | 663 | 22 |

Table 5.7 – Attack Categories, Sub-Classes, and Descriptions in NSL-KDD Dataset

| **Category** | **Sub-Class** | **Description** |
|---|---|---|
| DoS | Neptune | Floods victim with high traffic. |
| | Smurf | Spoofs victim's address in ICMP requests. |
| | Teardrop | Sends overlapping fragments. |
| | Pod | Floods victim with ICMP or UDP packets. |
| Probe | Nmap | Scanning tool for network discovery. |
| | Portsweep | Scans multiple ports on a host. |
| | Satan | Scanning tool for network reconnaissance. |
| | MScan | Scanner for identifying vulnerabilities. |
| R2L | Guess Password | Tries to guess user's password. |
| | FTP Write | Unauthorized write access to FTP server. |
| | IMAP Access | Unauthorized access to IMAP email server. |
| | Phf | Exploits "Phf" CGI vulnerability. |
| U2R | Buffer Overflow | Exploits buffer overflow vulnerabilities. |
| | Loadmodule | Loads kernel modules without proper privileges. |
| | Rootkit | Installs a rootkit on the victim system. |
| | Perl | Exploits vulnerabilities in Perl scripts. |

Table 5.8 – Confusion Matrix

| | Classified as Malicious | Classified as Honest |
|---|---|---|
| Classified as Malicious | True Positive (TP) | False Negative (FN) |
| Classified as Honest | False Positive (FP) | True Negative (TN) |

research in the field of network intrusion detection, making it an essential resource for studying network security and cyber threats. The primary purpose of the NSL-KDD dataset is to facilitate the development and evaluation of intrusion detection techniques. It serves as a valuable resource for researchers, data scientists, and security professionals who aim to build and test algorithms and models to identify various types of network intrusions and attacks.

— Dataset Size : The NSL-KDD dataset contains a substantial amount of network traffic data, with approximately 125,973 instances for training and 22,544 instances for testing. This diverse dataset allows for robust analysis and modeling.
— Data Variability : The dataset includes various types of benign and malicious network connections. It covers different attack types and strategies, offering a comprehensive view of potential security threats.
— Feature Set : NSL-KDD includes a rich set of features that describe network connections and behaviors, making it suitable for machine learning and data analysis. These features encompass aspects such as connection duration, protocol type, service, flags, byte counts, and more as shown in table 5.3 .
— Attack Categories : The dataset is categorized into several attack types, including Denial of Service (DoS), Probe, User to Root (U2R), and Remote to Local (R2L). This categorization allows for targeted analysis of specific types of attacks.
— Data Preprocessing : To address some of the issues present in the original KDD Cup 1999 dataset, the NSL-KDD dataset has undergone preprocessing to eliminate redundancy, correct inaccuracies, and provide a more realistic representation of network traffic.
— Testing and Evaluation : The dataset is divided into a training set and a testing set, enabling researchers to train models on one portion and evaluate their performance on another. This setup allows for fair testing and assessment of IDSs.

### 5.6.3 Attacks types

We present in this subsection a detailed descriptions to provide insights into the various attack classes and sub-classes present in the NSL-KDD dataset, highlighting the techniques and goals of different cyber threats.

#### 5.6.3.1 Denial of Service (DoS)

Neptune : The Neptune attack is a classic example of a Denial of Service attack. In this attack, the attacker floods the victim with a high volume of network traffic, typically to overwhelm the victim's resources, such as bandwidth or processing power, and make the service unavailable to legitimate users. Smurf : The Smurf attack involves ICMP (Internet Control Message Protocol) amplification, where the attacker sends ICMP requests with a spoofed source IP address to a network broadcast address. This results in multiple hosts responding to the victim, causing network congestion. Teardrop : Teardrop is an attack that sends intentionally overlapping IP fragments to a target system. When these fragments are reassembled, it can lead to buffer overflow or crashes in the victim's operating system. Pod : The Pod attack is a Denial of Service attack that involves flooding the victim with either ICMP or UDP packets. It aims to consume the target's resources and disrupt its normal operation.

#### 5.6.3.2 Probe

Nmap : Nmap is a popular open-source network scanning tool used for network discovery and security auditing. Attackers often use Nmap to identify open ports, services, and vulnerabilities on a target network. Portsweep : Portsweep is a scanning attack where the attacker probes multiple ports on a host, attempting to identify open ports and potential vulnerabilities. It is a common precursor to more specific attacks. Satan : Satan is another network scanning tool used for network reconnaissance. Attackers utilize Satan to gather information about a target network, including services, versions, and vulnerabilities. MScan : MScan is a scanner used to identify vulnerabilities in networked systems. It scans for specific weaknesses that could be exploited in later attacks.

#### 5.6.3.3 Remote to Local (R2L)

Guess Password : In this attack, the attacker attempts to gain unauthorized access to a system by guessing or cracking a user's password. It may involve dictionary attacks or brute force methods. FTP Write : The FTP Write attack involves unauthorized write access to an FTP (File Transfer Protocol) server. Attackers use this to upload malicious files or manipulate data on the server. IMAP Access : This

Table 5.9 – Environment setup

| Element | Description |
|---|---|
| OS | Windows 11 |
| CPU | 12th Gen Intel i7-1255U 1.70 GHz |
| RAM | 16G |
| Language | Python and Solidity |
| Dataset | NSL-KDD |
| IDE | Dataspell, Google Colab |
| Training Models | Federated Learning with MLP and RNN. |

attack involves unauthorized access to an IMAP (Internet Message Access Protocol) email server. Attackers may access, read, or modify emails without proper authorization. Phf : The Phf attack exploits the "Phf" CGI (Common Gateway Interface) vulnerability. It allows attackers to execute arbitrary commands on a target web server.

#### 5.6.3.4 User to Root (U2R)

Buffer Overflow : The Buffer Overflow attack involves exploiting vulnerabilities in software applications or operating systems where an attacker can overflow a buffer to execute malicious code or gain unauthorized access.

Loadmodule : In this attack, an attacker attempts to load kernel modules without proper privileges or authorization. This could allow them to modify the behavior of the operating system. Rootkit : A Rootkit is a collection of tools and software that an attacker installs on a victim system to gain unauthorized root-level access. Rootkits are used to hide the presence of malicious software or provide persistent access. Perl : Attackers may exploit vulnerabilities in Perl scripts, a widely used scripting language, to gain unauthorized access or execute malicious code on a target system. These detailed descriptions provide insights into the various attack classes and sub-classes present in the NSL-KDD dataset, highlighting the techniques and goals of different cyber threats.

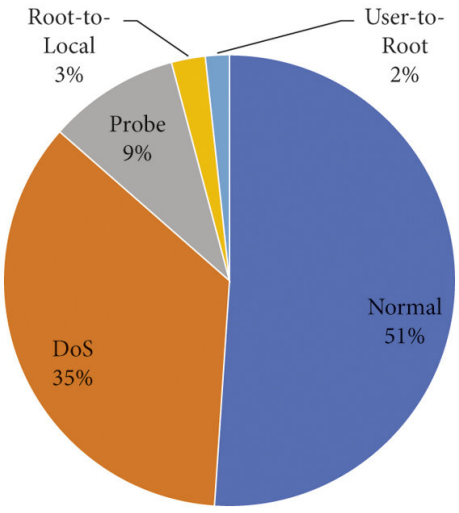



Figure 5.3 – NSL-KDD dataset distribution.

## 5.7 Results' Discussion

In this section, we discuss our extensive simulations' results of the VFed-IDS framework with the NSL-KDD dataset using both MLP and RNN models. We evaluate the robustness of the VFed-IDS metrics and then present the experimental results and analyze them in details as shown below.

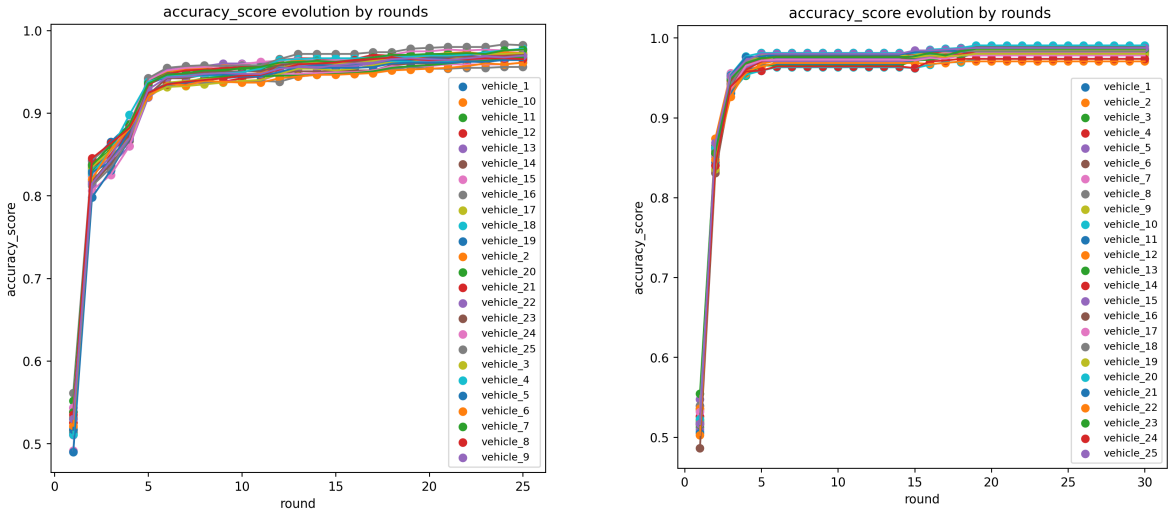
### 5.7.1 Impact of rounds number on model's metrics

The number of rounds affects the accuracy of the IDS model. More rounds typically lead to a more accurate model since it has more opportunities to learn from diverse data sources. However, there's a diminishing return on accuracy, and at a certain point, additional rounds may not significantly improve detection rates. Choosing the right number of rounds is about achieving a satisfactory level of accuracy without overburdening the system. Hence, we conduct extensive simulations in order to pick the right rounds number for each scenario. We illustrate the impact of varying the rounds numbers on the models' accuracy scores in most of the presented figures in this section.

#### 5.7.1.1 Accuracy

The accuracy score represents the overall correctness of the IDS's intrusion detection decisions. It is a typically used metric to assess the system's performance. Accuracy delivers a comprehensive measure of the IDS's performance by considering the correct detections and rejections. However, accuracy might not be the sole metric to consider, especially in scenarios with imbalanced datasets, where the number of non-intrusive instances significantly outweighs intrusions. A high accuracy score can be misleading in such cases, as the IDS might classify everything as non-intrusive. In practice, a balance between accuracy, precision, and recall is often sought, relying on the specific requirements and priorities of the IoV and the potential consequences of false alarms or missed intrusions. The choice of evaluation metrics should be made with a clear understanding of the system's objectives and the potential impact of its decisions on network security. The Accuracy score is calculated as follows :

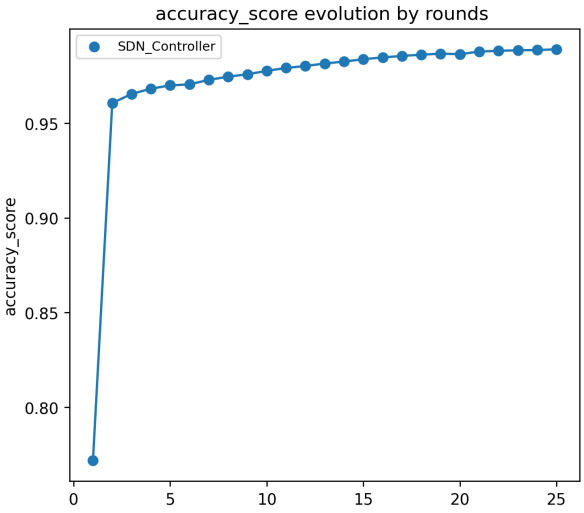
$$Accuracy = \frac{TN + TP}{TN + TP + FP + FN} \tag{5.6}$$



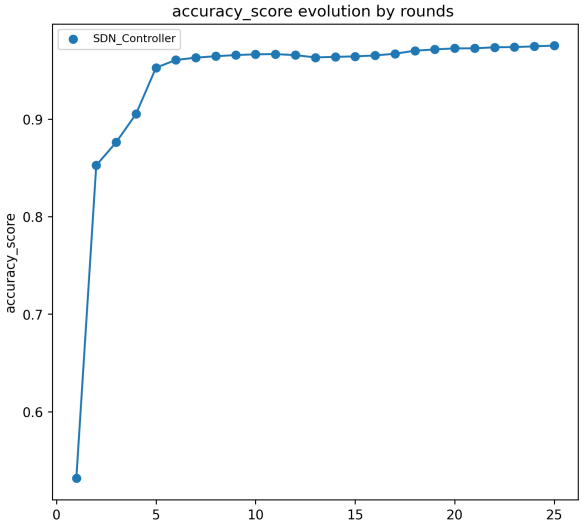

((a)) Accuracy rate of 25 vehicles with MLP model.

((b)) Accuracy rate of 25 vehicles with RNN model.

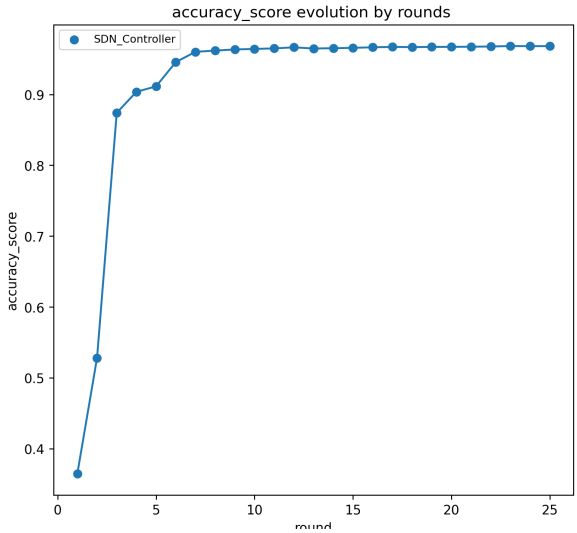
FIGURE 5.8 – Accuracy rate of 25 vehicles.



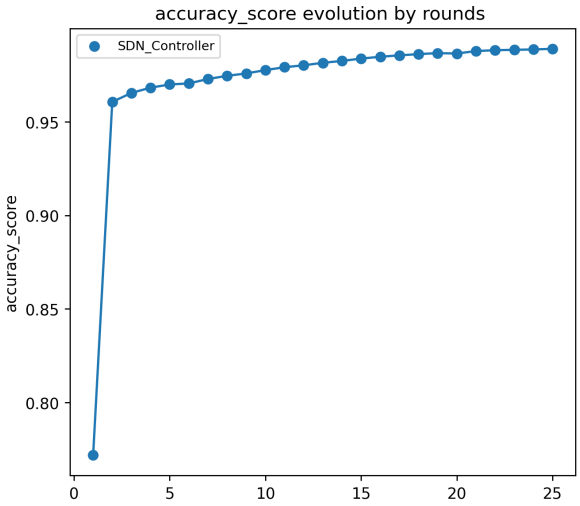

((a)) Accuracy rate of SDCN with 10 vehicles.




((b)) Accuracy rate of SDCN with 25 vehicles.

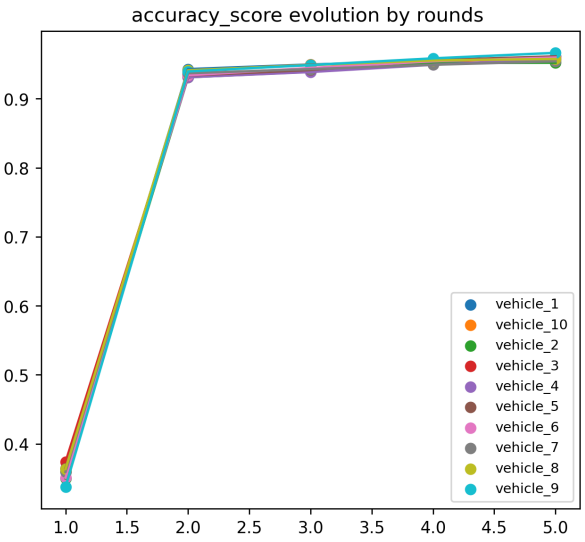



((c)) Accuracy rate of SDCN with 50 vehicles.

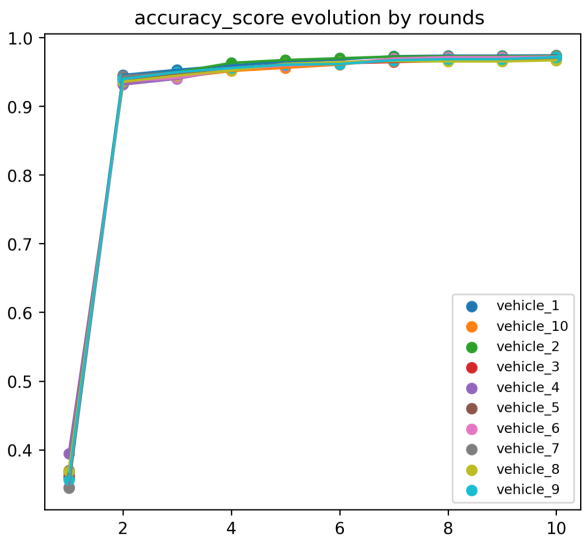



((d)) Accuracy rate of SDCN with 100 vehicles.

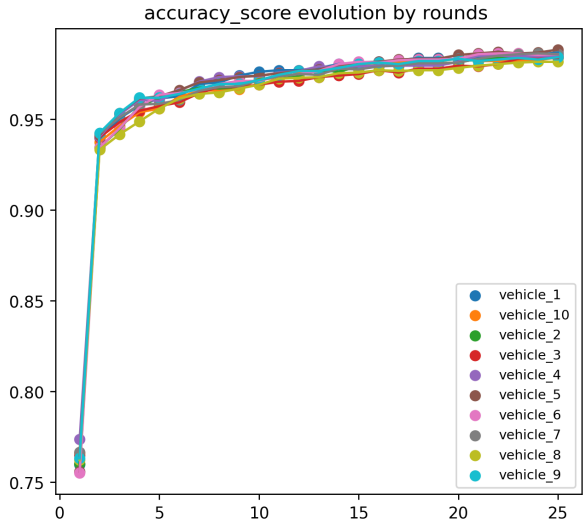
FIGURE 5.4 – Accuracy rate evolution of SDNC with MLP model while varying number of vehicles.



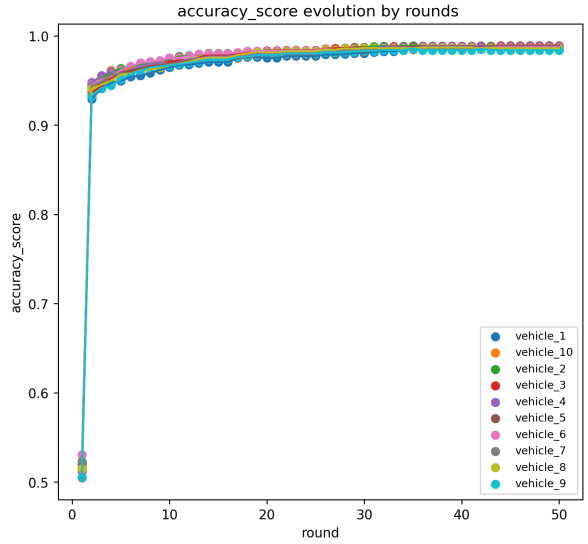

((a)) Accuracy rate of 10 vehicles in 5 rounds.




((b)) Accuracy rate of 10 vehicles in 10 rounds.

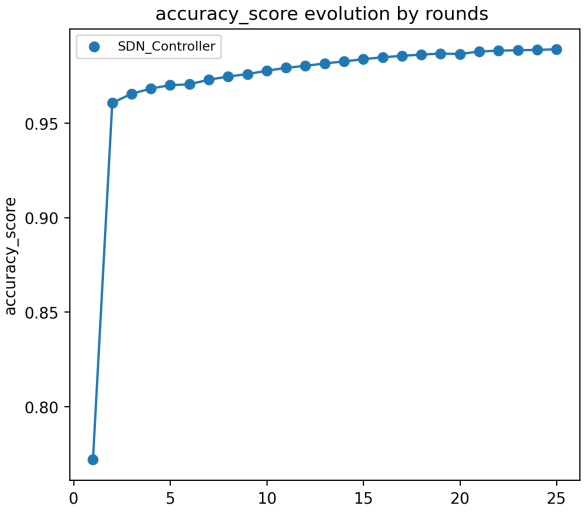



((c)) AAccuracy rate of 10 vehicles in 25 rounds.

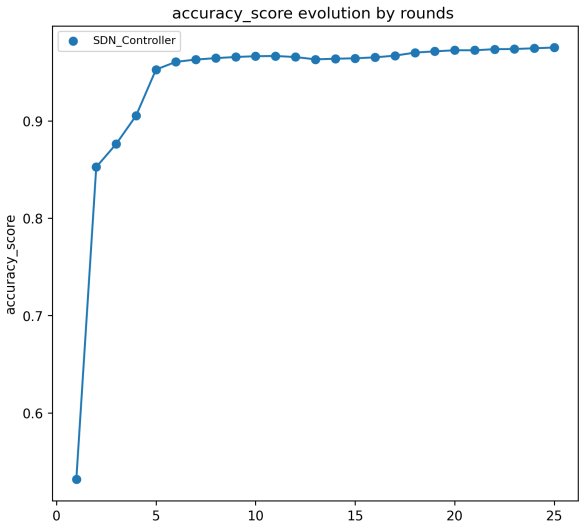



((d)) Accuracy rate of 10 vehicles in 50 rounds.

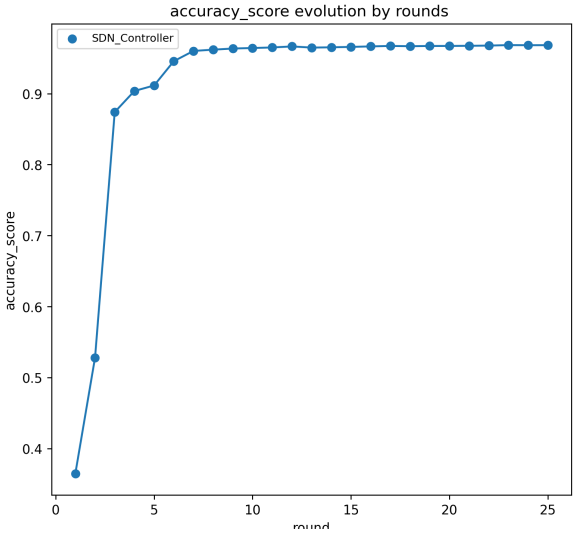
FIGURE 5.5 – Accuracy rate evolution of 10 vehicles with varying number of rounds.



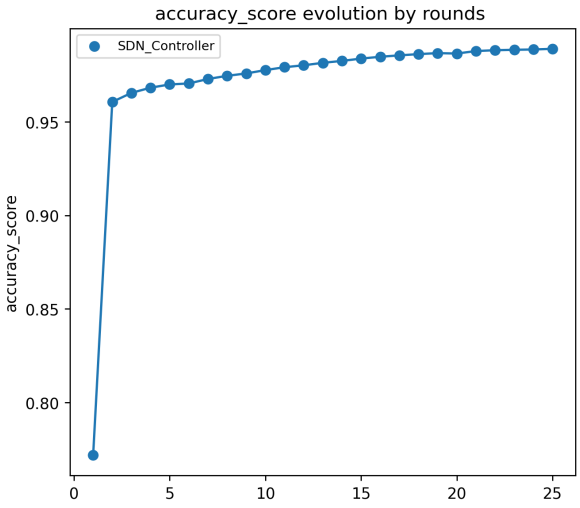

((a)) Accuracy rate of SDCN with 10 vehicles.




((b)) Accuracy rate of SDCN with 25 vehicles.

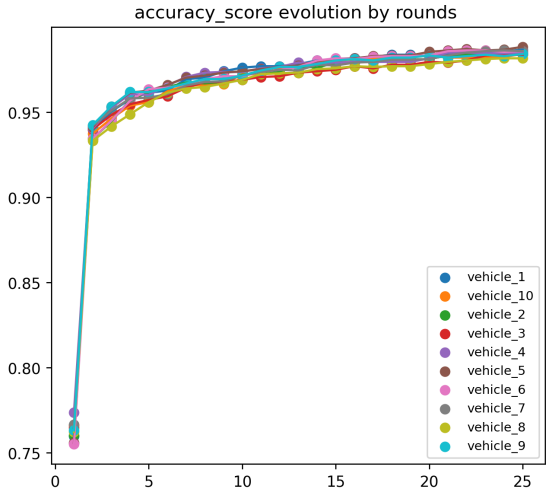



((c)) Accuracy rate of SDCN with 50 vehicles.

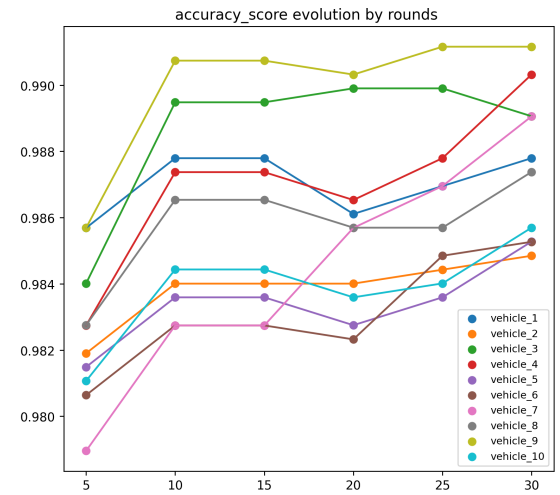



((d)) Accuracy rate of SDCN with 100 vehicles.

FIGURE 5.6 – Accuracy rate evolution of SDNC with varying number of vehicles.



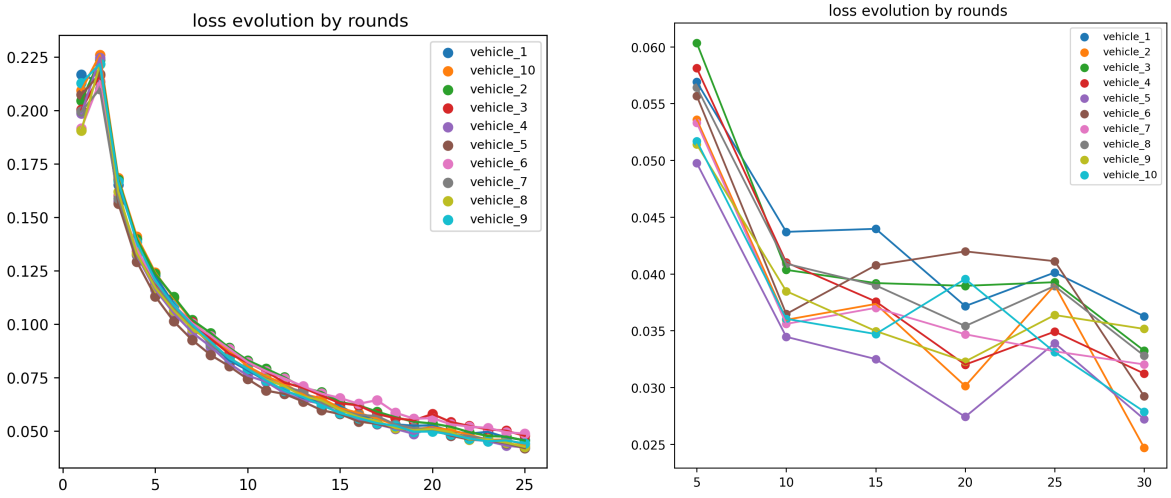

((a)) Accuracy rate of 10 vehicles with MLP model.




((b)) Accuracy rate of 10 vehicles with RNN model.

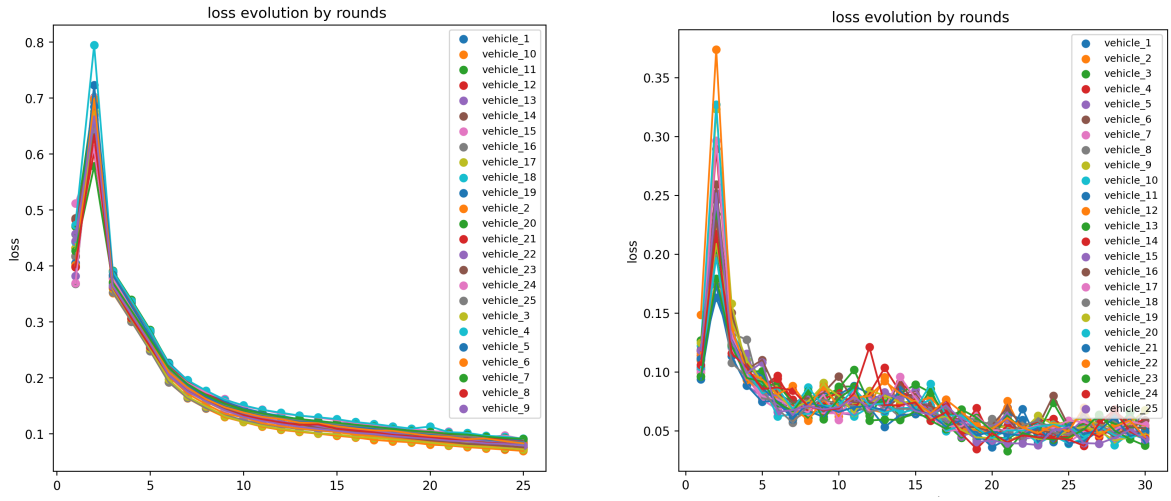
FIGURE 5.7 – Accuracy rate of 10 vehicles.

#### 5.7.1.2 Loss rate :




((a)) Loss rate of 10 vehicles with MLP model. ((b)) Loss rate of 10 vehicles with RNN model.

FIGURE 5.9 – Loss rate of 10 vehicles.




((a)) Loss rate of 25 vehicles with MLP model. ((b)) Loss rate of 25 vehicles with RNN model.

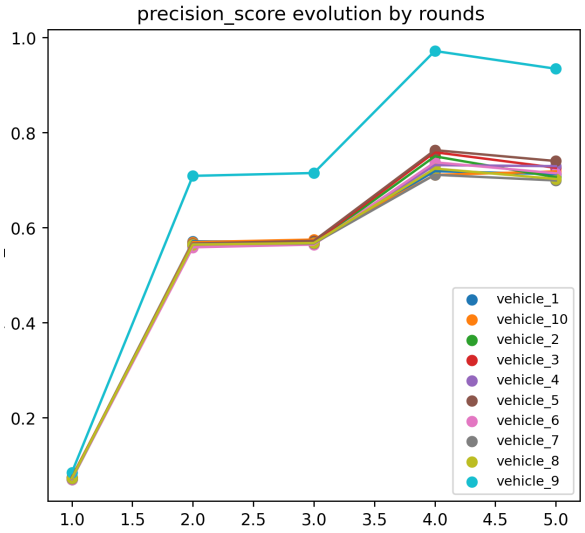
FIGURE 5.10 – Loss rate of 25 vehicles.

#### 5.7.1.3 Precision

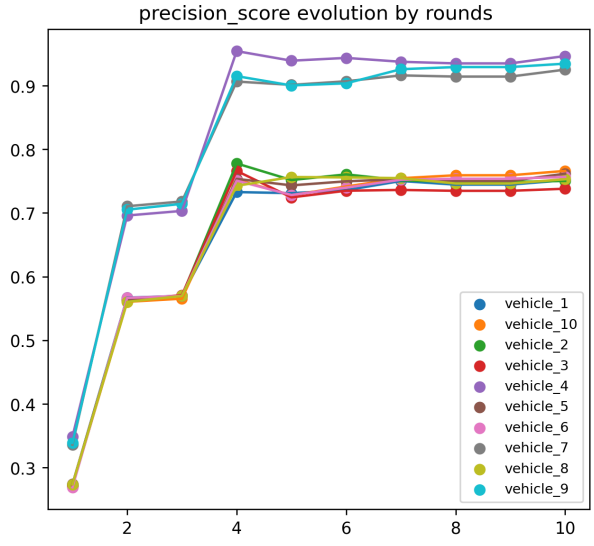
The precision represents the proportion of correctly detected intrusions by the IDS out of all the instances it flagged as intrusions. It measures the accuracy of the IDS in correctly identifying intrusions while minimizing false positives, which are instances where the IDS incorrectly identifies normal behavior as an intrusion. The Precision score is calculated as given below :

$$Precision = \frac{TP}{TP + FP} \tag{5.7}$$

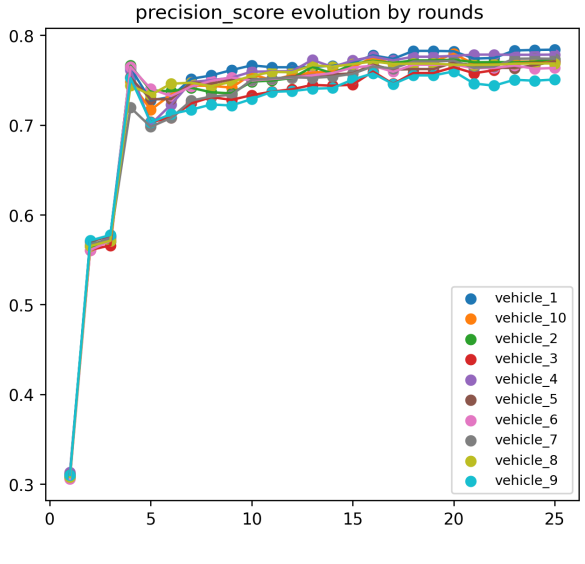
Where TP is the True Positives and FP is the False Positives.



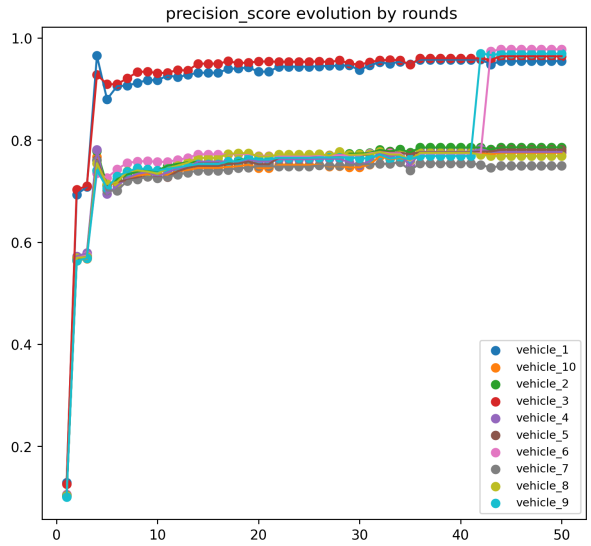

((a)) Precision score for 10 vehicles, 5 rounds, 5 epoch.




((b)) Precision score for 10 vehicles, 10 rounds, 5 epoch.

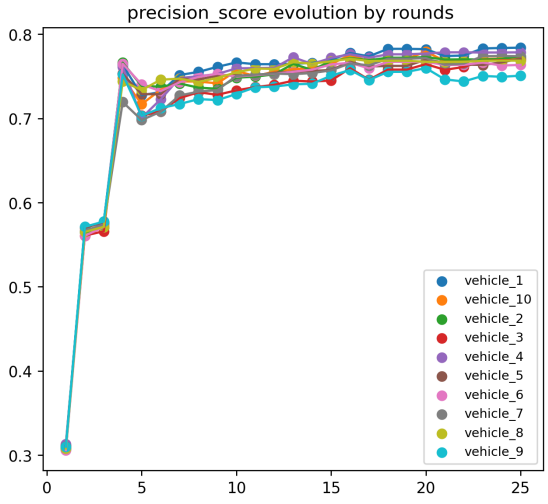



((c)) Precision score for 10 vehicles, 25 rounds, 5 epoch.

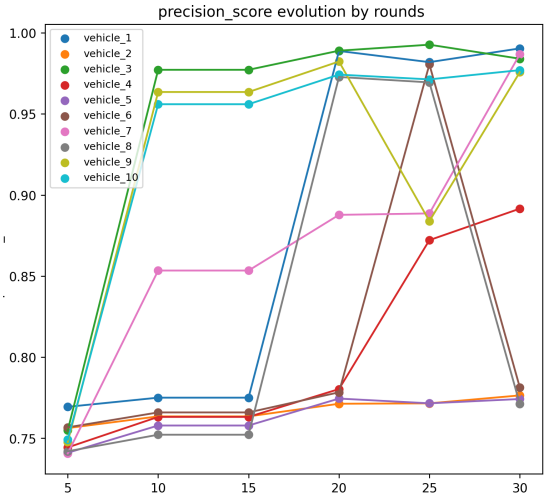



((d)) Precision score for 10 vehicles, 50 rounds, 5 epoch.

FIGURE 5.11 – Precision score evolution of vehicles per rounds with MLP model.

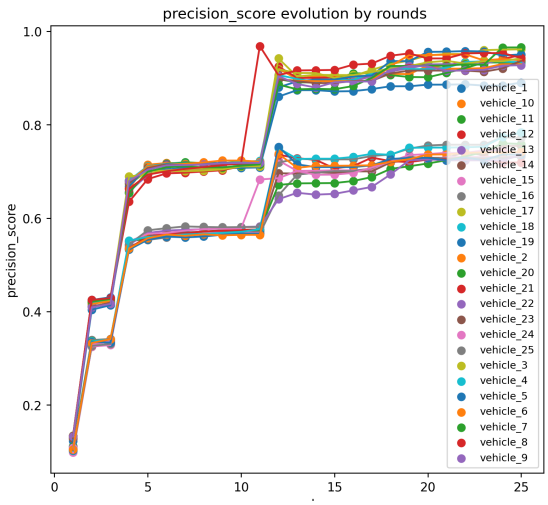



((a)) Precision scores of 10 vehicles with MLP model.

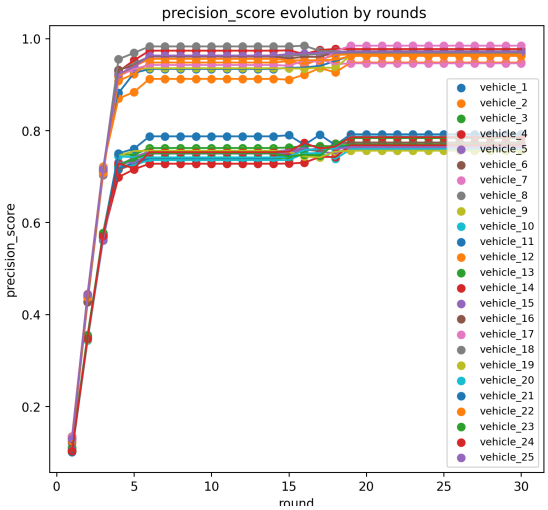



((b)) Precision scores of 10 vehicles with RNN model.

FIGURE 5.12 – Precision scores of 10 vehicles with MLP and RNN models.




((a)) Precision scores of 25 vehicles with MLP model.




((b)) Precision scores of 25 vehicles with RNN model.

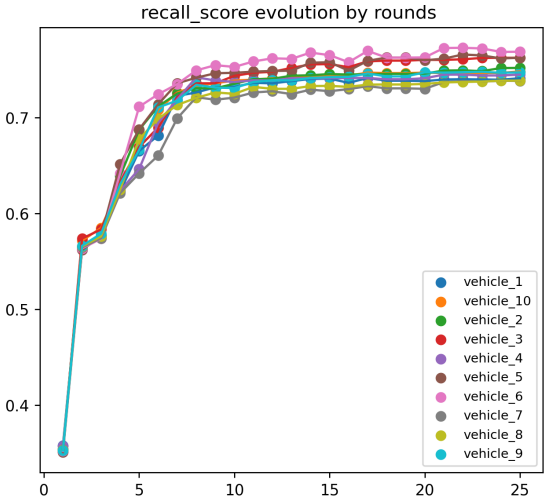
FIGURE 5.13 – Precision scores of 25 vehicles with MLP and RNN models.

#### 5.7.1.4 Recall

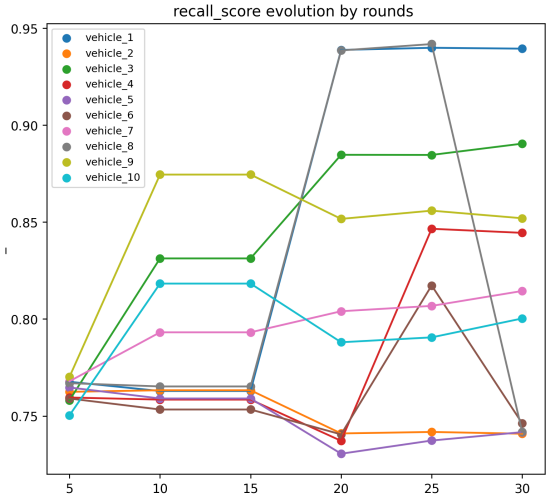
The recall score, also referred to as sensitivity or true positive rate (TPR), signifies the ratio of true intrusions or attacks correctly identified by the intrusion detection system. It quantifies the system's effectiveness in detecting real intrusions out of the total occurrences of intrusions. A high recall score indicates that the IDS effectively identifies many intrusions, which is vital for security in the IoV because missing intrusions can lead to severe network security and safety consequences. Therefore, a high recall score is desirable in an IDS for vehicular networks. Nevertheless, it should be balanced with other metrics like precision (to minimize false alarms) and F1 score to ensure the overall effectiveness of the IDS. The Recall score is calculated depending on the following equation :

$$Recall = \frac{TP}{TP + FN} \tag{5.8}$$

Where : TP is True Positives and FN is the False Negatives.

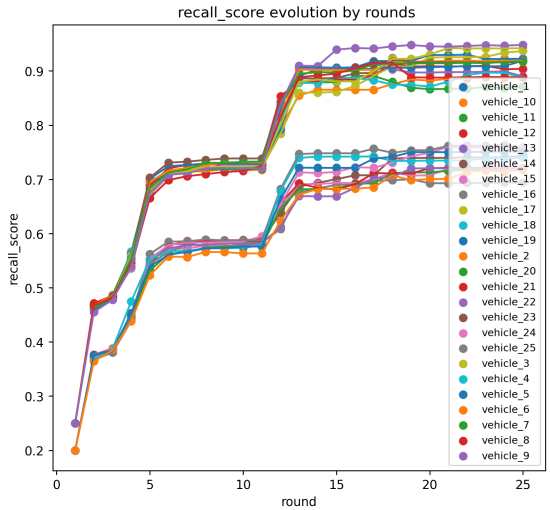



((a)) Recall scores of 10 vehicles with MLP model.

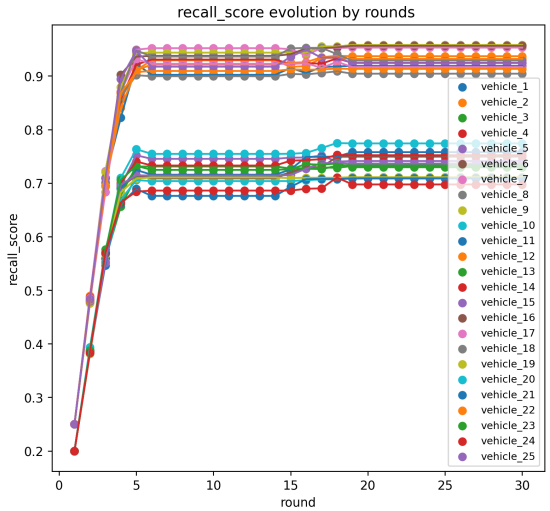



((b)) Recall scores of 10 vehicles with RNN model.

FIGURE 5.14 – Recall scores of 10 vehicles with MLP and RNN models.

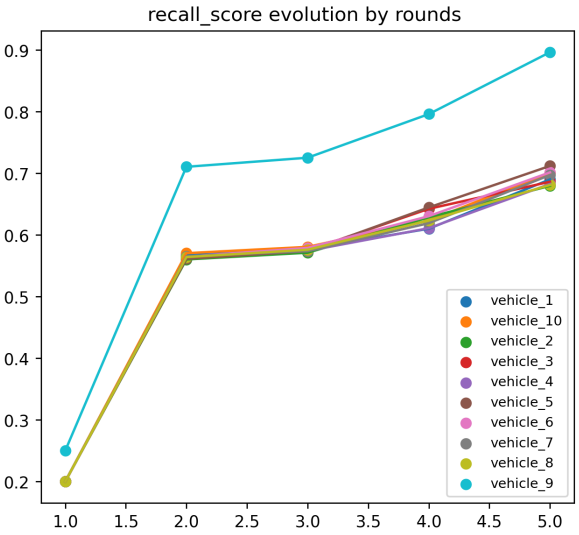



((a)) Recall scores of 25 vehicles with MLP model.

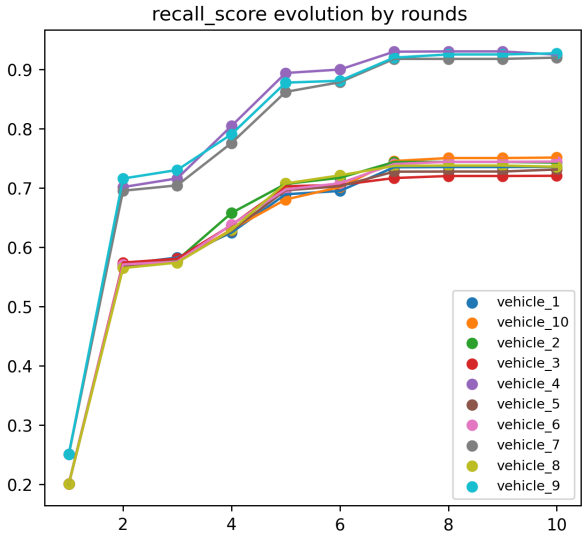



((b)) Recall scores of 25 vehicles with RNN model.

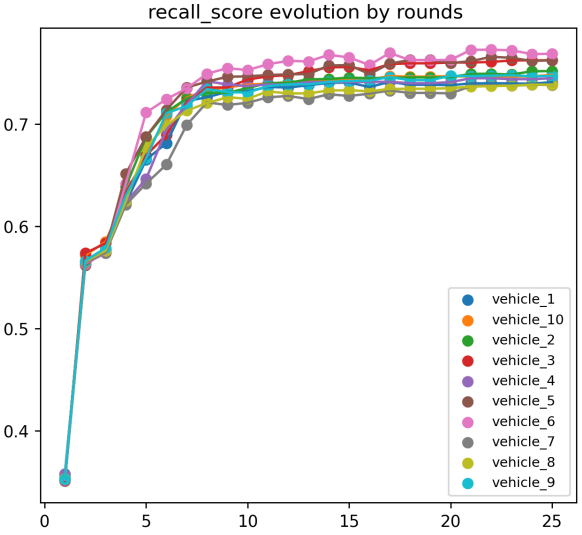
FIGURE 5.15 – Recall scores of 25 vehicles with MLP and RNN models.

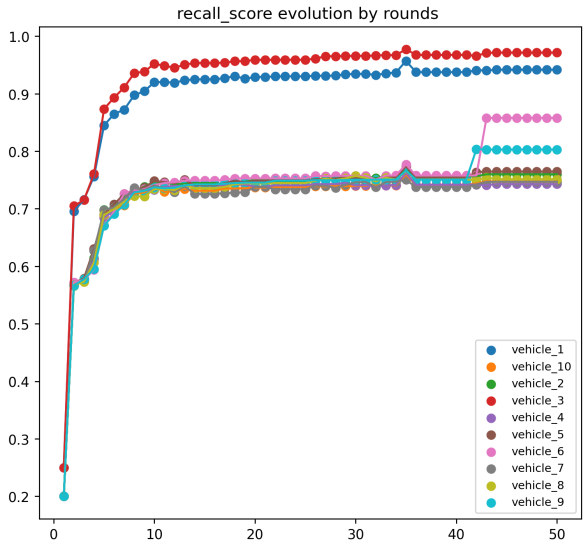



((a)) F1 scores for 10 vehicles, 5 rounds, 5 epoch.



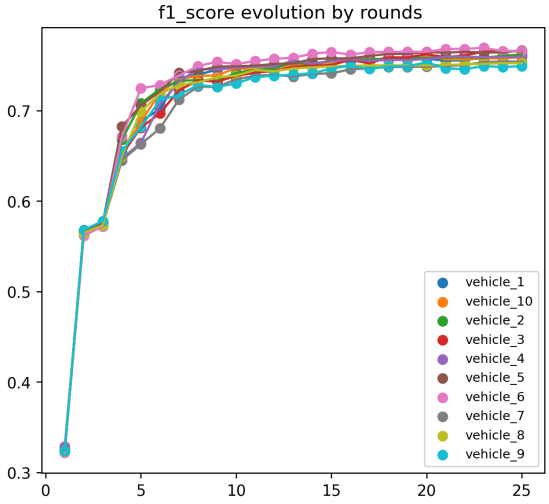

((b)) Loss function for 10 vehicles, 10 rounds, 5 epoch.



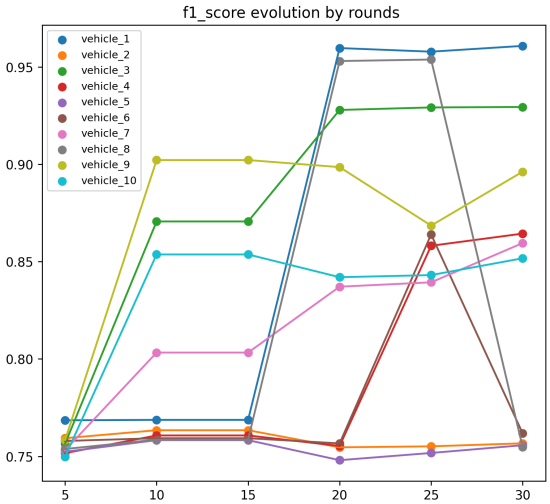




((c)) Loss function for 10 vehicles, 50 rounds, 5 epoch.

FIGURE 5.16 – Recall Score evolution of vehicles per rounds.

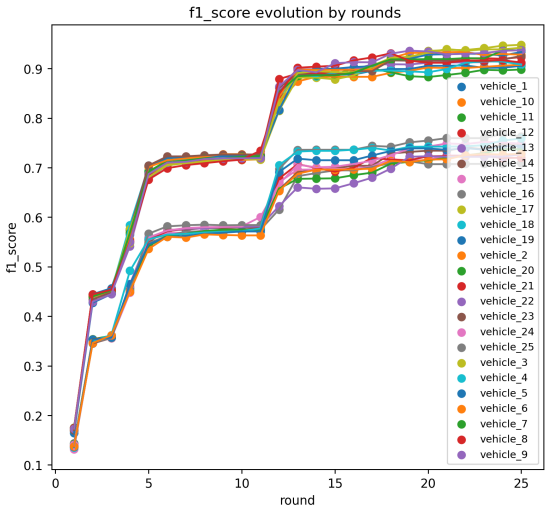



((a)) F1 scores of 10 vehicles with MLP model.

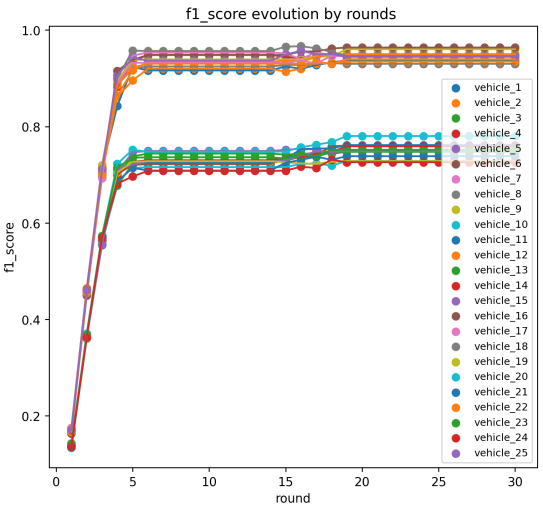



((b)) F1 scores of 10 vehicles with RNN model.

FIGURE 5.17 – F1 scores of 10 vehicles.




((a)) F1 scores of 25 vehicles with MLP model.



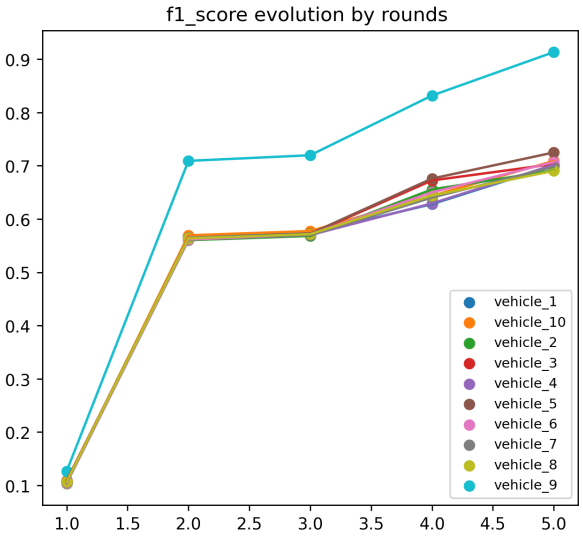

((b)) F1 scores of 25 vehicles with RNN model.

FIGURE 5.18 – F1 scores of 25 vehicles.

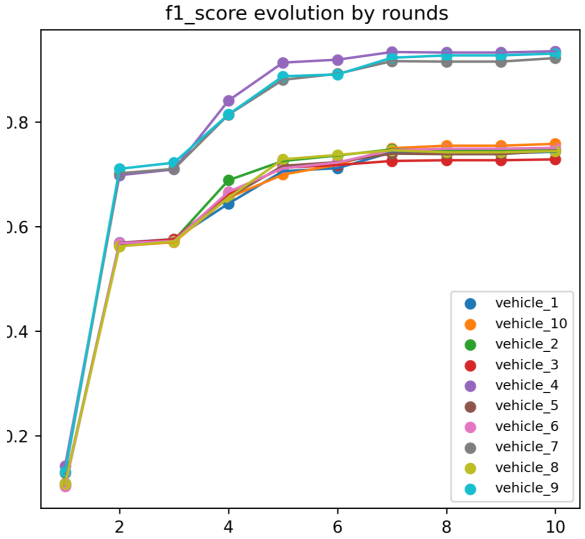
#### 5.7.1.5 F1-score

The F1 rate or F1 score, also known as the F-measure, serves as a metric for evaluating the overall performance of an Intrusion Detection System (IDS), taking into account both precision and recall. The F1 score is valuable in striking a balance between minimizing false alarms (precision) and ensuring that actual intrusions are not overlooked (recall). Ranging from 0 to 1, a higher F1 score indicates better performance. Its maximum value of 1 is achieved when precision and recall are optimized. The F1 score is significant in scenarios where achieving a balance between precision and recall is essential. For an IDS in the IoV, this means effectively detecting intrusions while keeping false alarms to a minimum. Striking this balance is essential to guarantee that security incidents are accurately identified without causing unnecessary disruptions or wasting resources on false positives. The F1 score is a valuable way to evaluate and compare IDS performance in such cases. The F1 score is calculated as below :

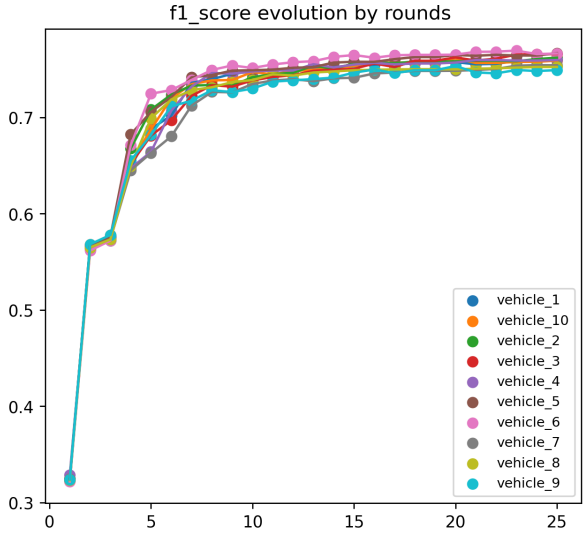
$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{5.9}$$



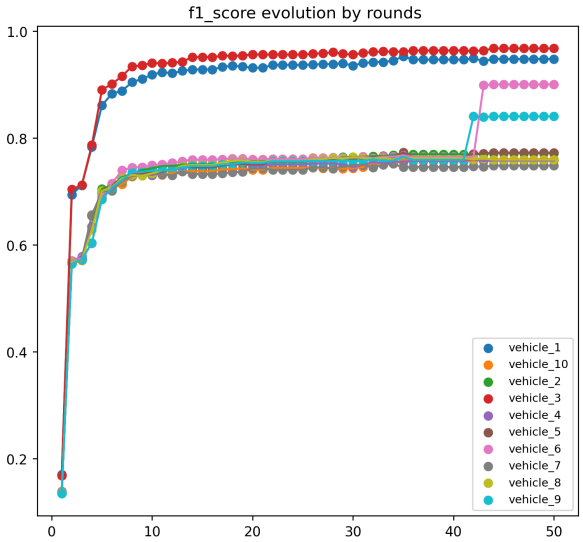

((a)) F1 scores for 10 vehicles, 5 rounds, 5 epoch.




((b)) F1 scores for 10 vehicles, 10 rounds, 5 epoch.

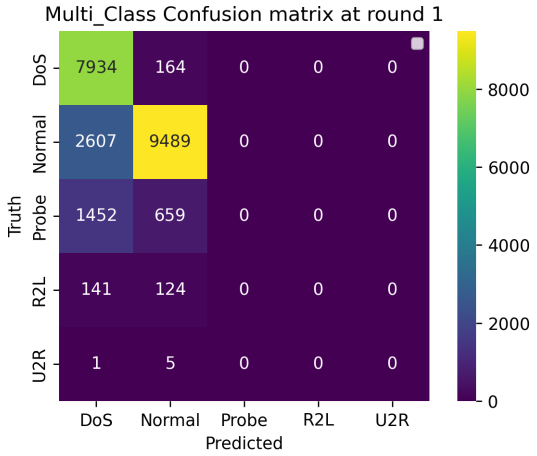



((c)) F1 scores for 10 vehicles, 25 rounds, 5 epoch.

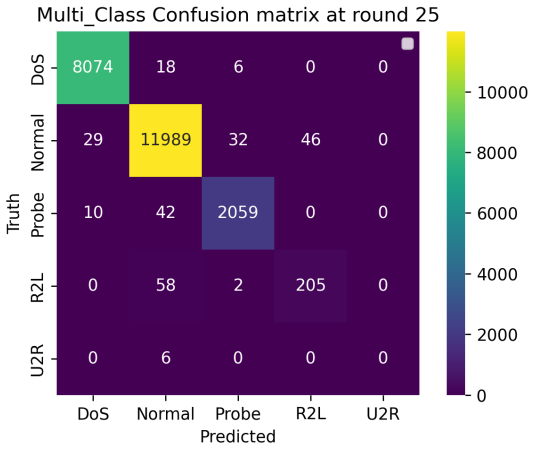



((d)) F1 scores for 10 vehicles, 50 rounds, 5 epoch.

FIGURE 5.19 – F1 score evolution of vehicles per rounds with MLP model.

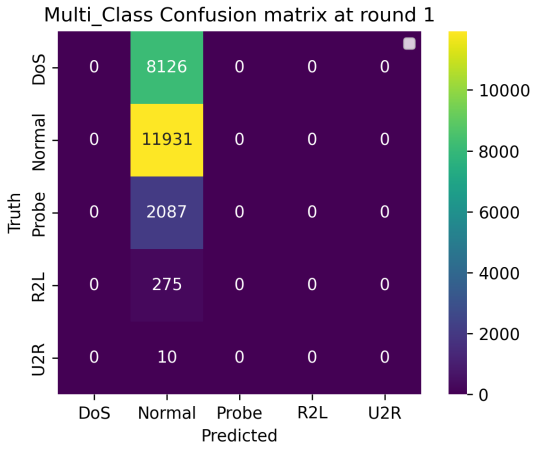



((a)) SDNC Confusion Matrix at first round.

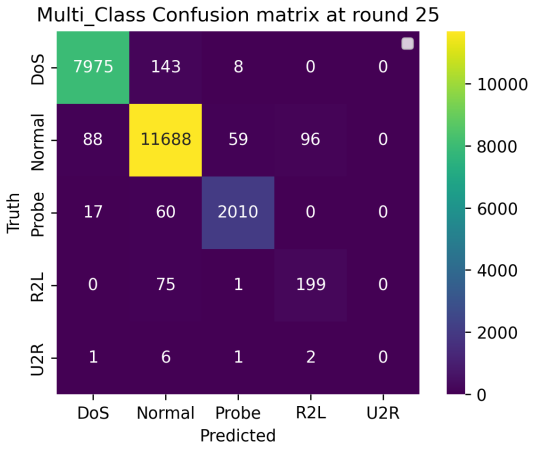



((b)) SDNC Confusion Matrix at last round.

FIGURE 5.20 – SDNC Confusion Matrix evolution with 10 vehicles with MLP model.

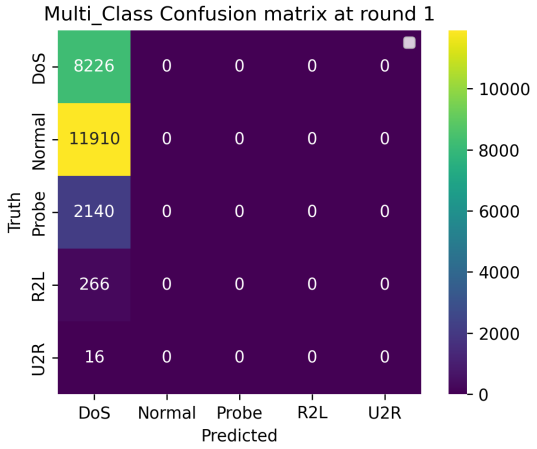



((a)) SDNC Confusion Matrix at first round.

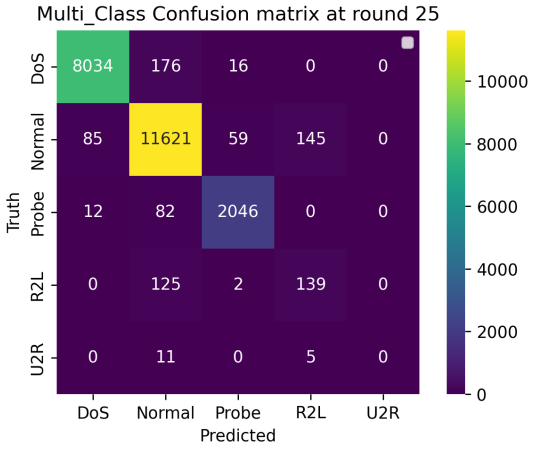



((b)) SDNC Confusion Matrix at last round.

FIGURE 5.21 – SDNC Confusion Matrix evolution with 25 vehicles with MLP model.

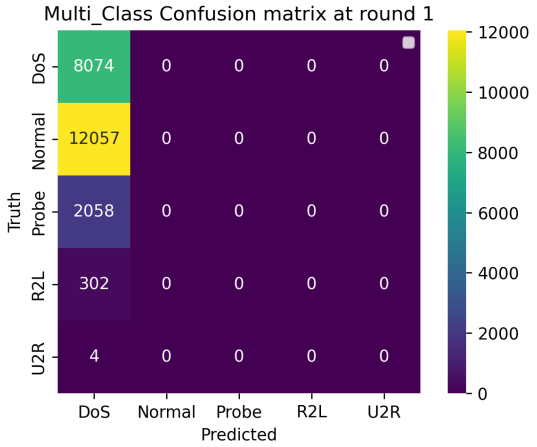



((a)) SDNC Confusion Matrix at first round.

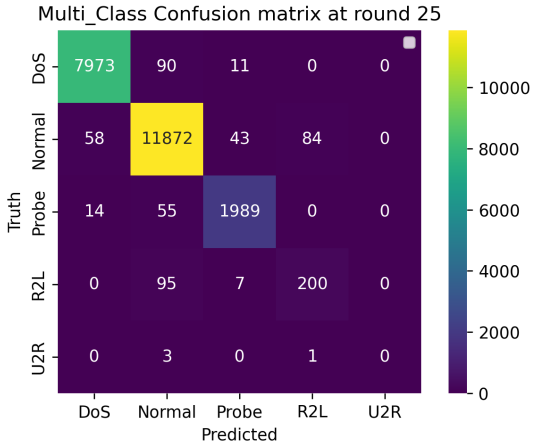



((b)) SDNC Confusion Matrix at last round.

FIGURE 5.22 – SDNC Confusion Matrix evolution with 50 vehicles with MLP model.

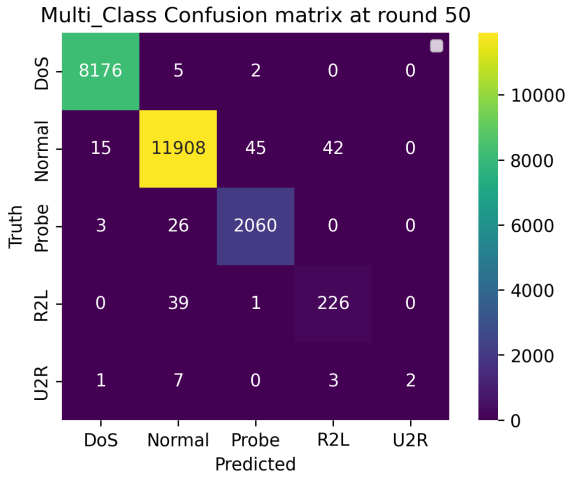



((a)) SDNC Confusion Matrix at first round.

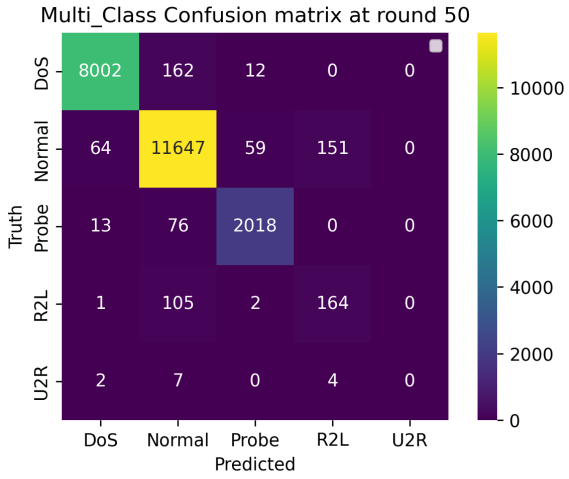



((b)) SDNC Confusion Matrix at last round.

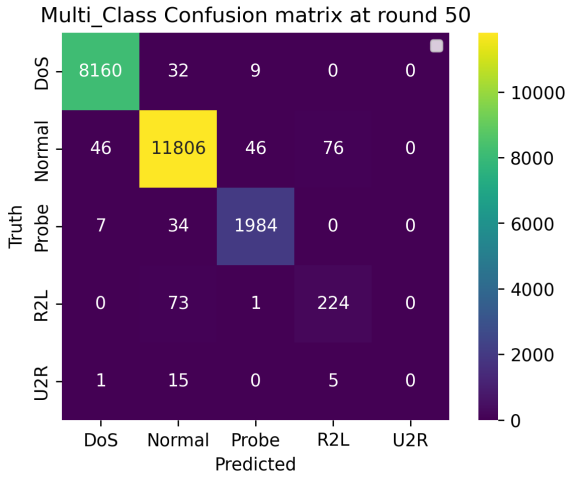
FIGURE 5.23 – SDNC Confusion Matrix evolution with 100 vehicles with MLP model.



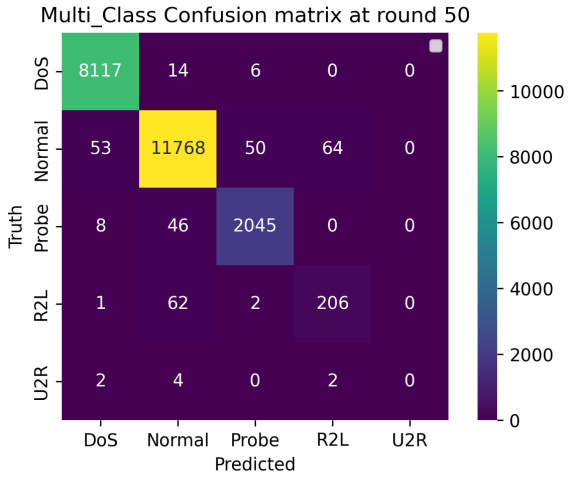

((a)) Accuracy rate of SDCN with 10 vehicles.




((b)) Accuracy rate of SDCN with 25 vehicles.




((c)) Accuracy rate of SDCN with 50 vehicles.

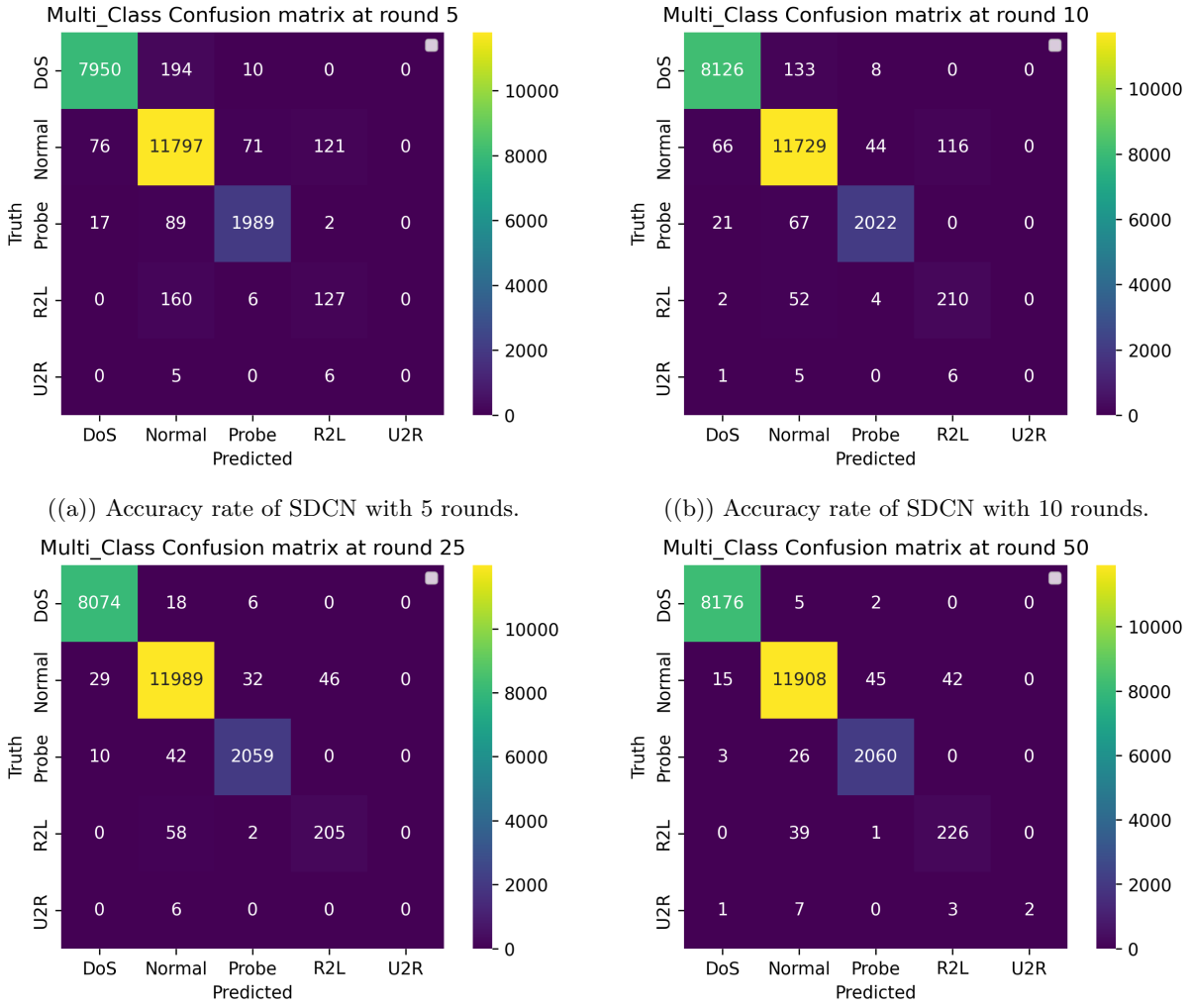



((d)) Accuracy rate of SDCN with 100 vehicles.

FIGURE 5.24 – SDNC Confusion Matrixes' Evolution with MLP model while varying vehicles' number.

As shown in the following sub-figures, increasing the number of rounds permits the VFed-IDS to classify correctly a bigger number of attacks at each scenario.therefore, the number of attacks classified as DoS correctly increases with 226 after varying the rounds number from 5 to 50. The number of attacks

classified as Probe correctly increases with 71. Also, the number of attacks classified as R2L correctly increases with 99. Moreover, the normal traffic classified correctly as normal increases with 211. We can notice that our framework couldn't classify any U2R attack correctly with 5 rounds of training. However, it classified correctly 2 attacks regardless the few number of U2R examples (only 119 records) in the NSL-KDD dataset.




((a)) Accuracy rate of SDCN with 5 rounds.

((b)) Accuracy rate of SDCN with 10 rounds.

((c)) Accuracy rate of SDCN in 25 rounds.

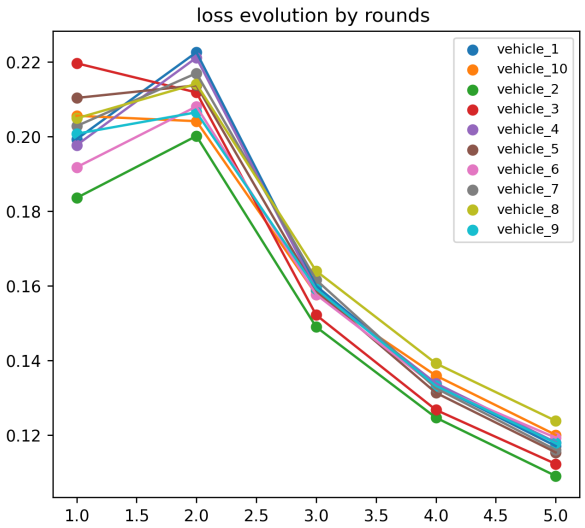
((d)) Accuracy rate of SDCN in 50 rounds.

FIGURE 5.25 – SDNC Confusion Matrixes' Evolution with MLP model while varying rounds' number.

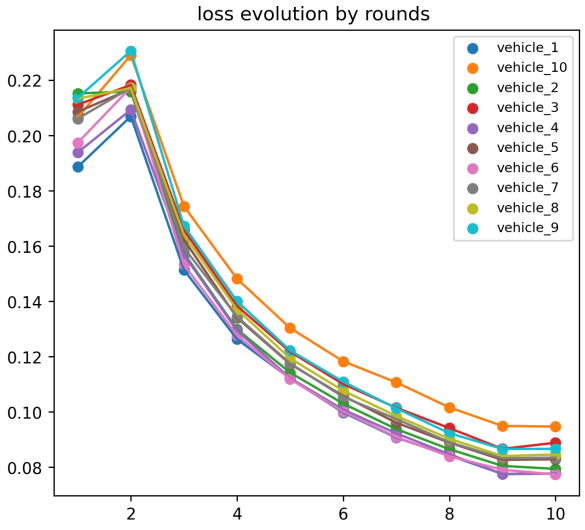
The results of our contribution are called VFed results. The VFed results that were executed on the whole NSL-KDD dataset are detailed in this section. The levels of accuracy are shown in Figure 5.23. The RNN model provides the best accuracy for FL with (99%) and (98%) with the MLP model. These accuracy levels were (78%) and (81%) respectively, with a ML approach. The use of the FL approach is very beneficial in terms of privacy preservation ; however, it can decrease the accuracy level due to FL's distrusted behavior. Figure 5.22 outlines the accuracy scores of VFed-IDS compared to other ML/DL models. The figure shows that our framework provides the highest accuracy rate with preserving the privacy of users.

### 5.7.2 ROC Curve

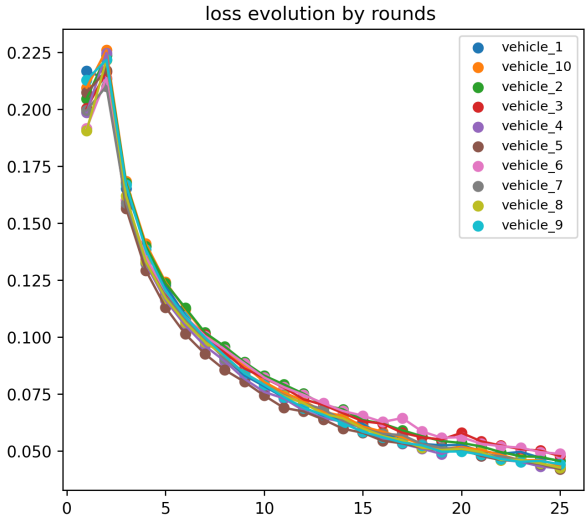
A Receiver Operating Characteristic (ROC) curve is a graphical representation employed to assess the performance of a binary classification model, such as our Intrusion Detection System (IDS). The ROC curve visually illustrates the trade-off between the true positive rate (sensitivity) and the false positive rate (1-specificity) at various threshold values for the classification model. This graphical representation enables a visual assessment of the IDS's performance. A curve that approaches the top-left corner of the plot indicates a more effective system, achieving higher true positive rates while keeping false positive



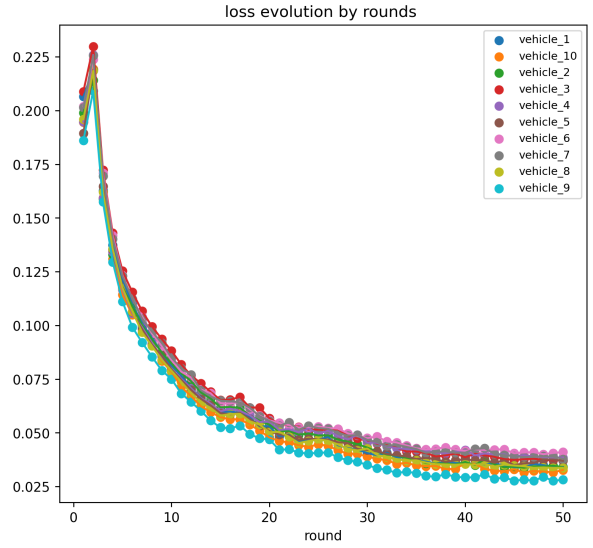

((a)) Loss function for 10 vehicles, 5 rounds, 5 epoch.




((b)) Loss function for 10 vehicles, 10 rounds, 5 epoch.




((c)) Loss function for 10 vehicles, 25 rounds, 5 epoch.




((d)) Loss function for 10 vehicles, 50 rounds, 5 epoch.

FIGURE 5.26 – Loss rate evolution of 10 vehicles varying rounds number with MLP model.

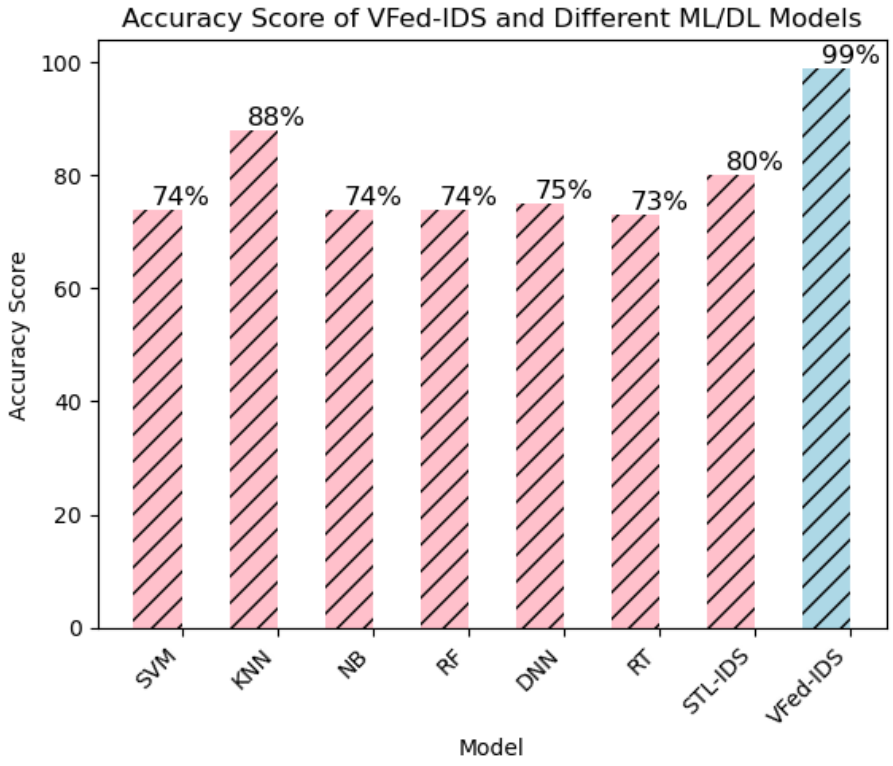



FIGURE 5.27 – Accuracy Score of VFed-IDS and other ML/DL models.

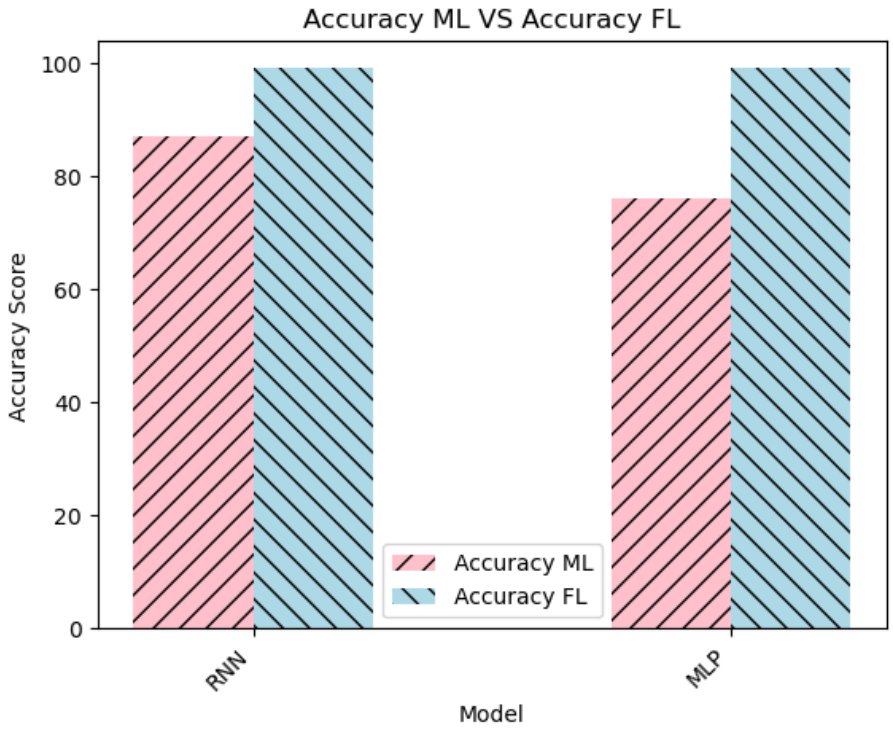
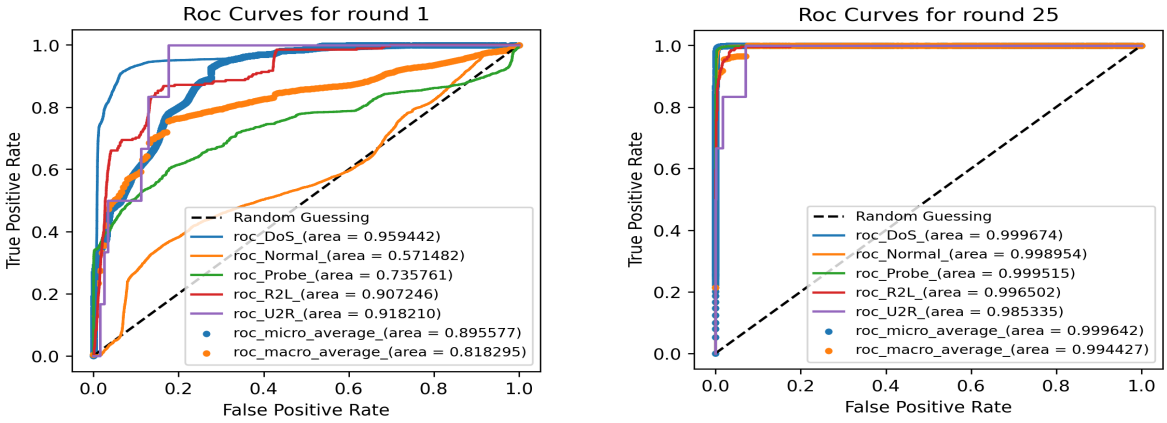



FIGURE 5.28 – The VFed and ML accuracy results of MLP and RNN models.




((a)) ROC Curve at first round.

((b)) ROC curve at last round.

FIGURE 5.30 – ROC Curve Evolution of SDNC with 10 vehicles in 25 rounds with MLP model.

rates low, as depicted in the following figure.

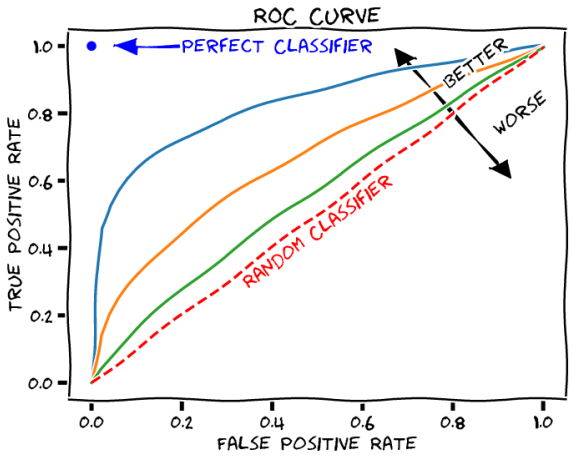
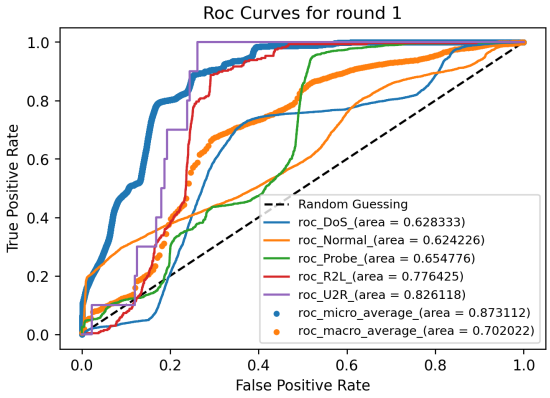
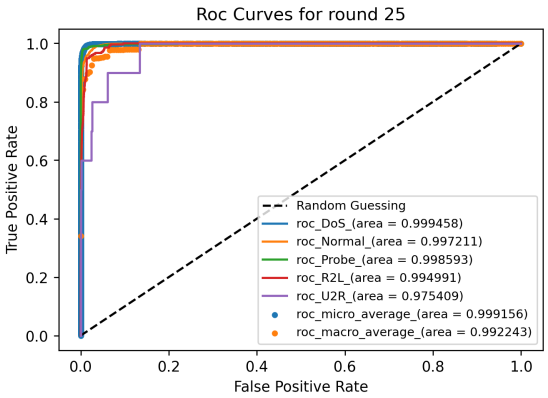



FIGURE 5.29 – The ROC Curve concept.

We conducted extensive simulations in this contribution, demonstrating that our proposed VFed-IDS shows perfect ROC curves in different scenarios, as illustrated in figure 5.25, figure 5.26, figure 5.27, and figure 5.28. As shown in presented ROC curves, we tested our framework with a large number of vehicles up to 100. We launched multiple simulations with both MLP and RNN model where we varied the number of vehicles and fixed other parameters like the rounds numbers, epoch value, batch-size value. The VFed-IDS makes it a perfect solution to cope with scalability issues in IDS in the IoV. Hence, the VFed-IDS is a robust and adaptive security solution for detecting cyber threats in the IoV. Achieving a perfect ROC curve signifies outstanding detection capabilities, where the VFed-IDS simultaneously provides high sensitivity and specificity. It is highly effective at identifying intrusions while keeping false alarms to an absolute minimum. This level of accuracy ensures timely responses to security incidents. The VFed-IDS assures high security by detecting all intrusions without raising any false alarms, which enhances vehicular network users' safety since a single missed intrusion or a false alarm can have severe consequences. The VFed-IDS does not disrupt network operations with false alarms, which reduces the need for manual intervention to investigate or filter out false positives, saving time and enhancing the resources' consumption by not wasting resources on false alarms or redundant alerts. Investigating false alarms or responding to missed intrusions is significantly reduced by the proposed IDS, which makes a cost-saving solution regarding incident response and operational overhead.

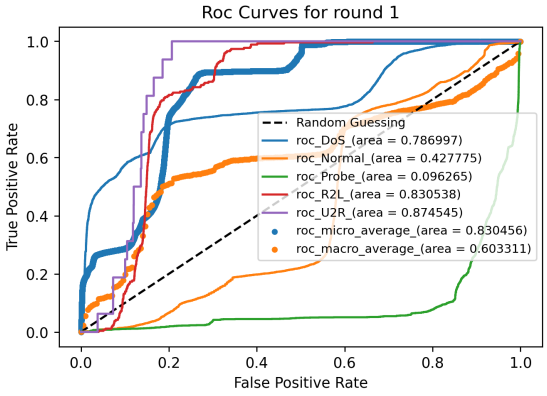



((a)) ROC Curve at first round.

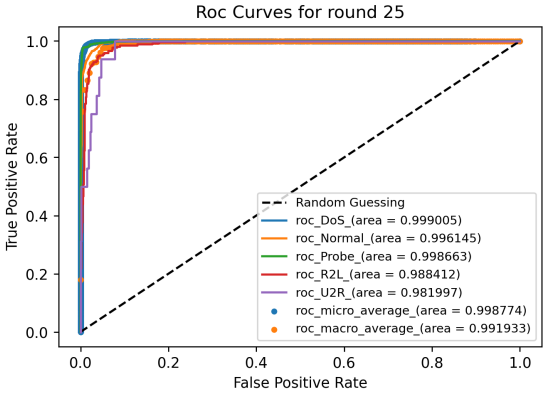



((b)) ROC curve at last round.

FIGURE 5.31 – ROC Curve Evolution of SDNC with 25 vehicles in 25 rounds with MLP model.

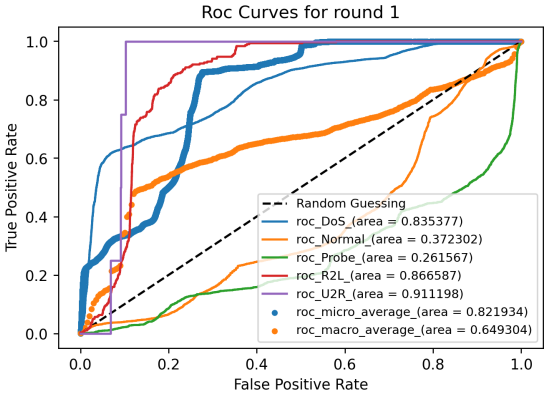



((a)) ROC Curve at first round.

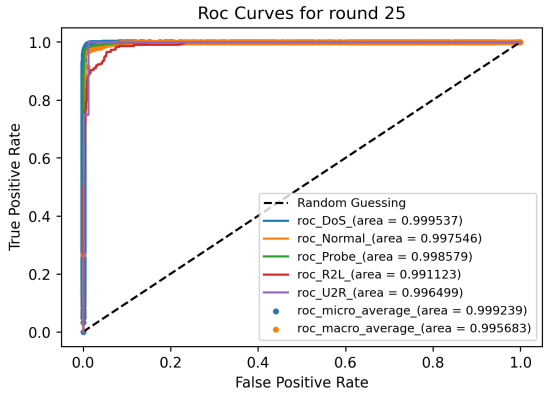



((b)) ROC curve at last round.

FIGURE 5.32 – ROC Curve Evolution of SDNC with 50 vehicles in 25 rounds with MLP model.




((a)) ROC Curve at first round.




((b)) ROC curve at last round.

FIGURE 5.33 – ROC Curve Evolution of SDNC with 100 vehicles in 25 rounds with MLP model.

–

## 5.8 Open issue

### 5.8.1 Federated Learning Clients' Selection

In IoV, carefully curating FL clients is pivotal in optimizing the collaborative training process among interconnected vehicles. The FL process entails a collective effort where numerous vehicles, acting as

clients, jointly train a shared machine-learning model. Crucially, this is achieved while maintaining the integrity of each vehicle's decentralized data, thus upholding privacy and security standards. Selecting FL clients in the context of IoV is a multifaceted undertaking. Factors that necessitate thoughtful consideration encompass the availability of locally relevant data, the computational capabilities inherent to each vehicle, and their current network connectivity status. Efficient client selection ensures that only those vehicles possessing pertinent data actively contribute to the model training endeavor. This approach is instrumental in curtailing superfluous communication overhead and, notably, in conserving the limited bandwidth resources characteristic of IoV or vehicular networks. Furthermore, these networks' dynamic and real-time nature requires a client selection process that adapts to shifting network conditions and evolving vehicle participation. As a result, this dynamic approach emerges as a critical element, significantly augmenting the performance and accuracy of the machine learning models deployed in diverse vehicular applications, such as intelligent traffic management and the advancement of road safety. In the broader FL context, integration into the training of a global model through a distributed architecture maintains data privacy. However, due to the many clients involved, effective selection mechanisms are necessary. These mechanisms must address the diversity among clients, including variations in system configurations and available data, which, if not managed appropriately, can lead to inefficiencies in the training process. Therefore, revising traditional client selection methods is imperative to harness the potential of FL in such heterogeneous environments effectively [177].

### 5.8.2 Rounds' total number of FL process

Intrusion detection systems in the IoV are powered by FL. This collaborative approach safeguards the privacy of vehicular data while enabling collective model training. The efficiency and effectiveness of FL in IoV-based IDS are intricately tied to the number of rounds the FL process encompasses. These rounds signify the iterative stages where FL clients, represented by vehicles, engage in model updates and aggregations. The total number of rounds in the FL process serves as a critical parameter that directly impacts the convergence and accuracy of the IDS model. The delicate balance between training accuracy and the consumption of network and computational resources guides the careful selection of this parameter. A higher number of rounds typically leads to a more refined model and heightened detection accuracy, allowing for extensive data exchanges and collaborative learning. However, this comes at the cost of prolonged communication and computation times, which can strain the resources of connected vehicles and the IoV network. Conversely, fewer rounds are preferred for expediency and resource conservation, albeit at the expense of detection precision. Therefore, determining the total number of FL rounds in IoV-based IDS necessitates meticulously considering the network's dynamics, computational capacities of vehicles, and the trade-off between model accuracy and resource consumption. Striking the right balance in round selection is essential to ensure the IDS system's overall efficiency, responsiveness, and ability to promptly and accurately identify and mitigate security threats within the ever-evolving and interconnected landscape of IoV. Therefore, as part of future research, our focus will be on developing intelligent algorithms that adaptively adjust the number of rounds in the Federated Learning (FL) process based on real-time network conditions, vehicular participation, and model convergence. This dynamic approach aims to enhance the efficiency of Intrusion Detection Systems (IDS) in the context of the Internet of Vehicles (IoV), ensuring that detection accuracy is maintained and improved. This is crucial as the number of training rounds directly impacts resource utilization.

## 5.9 Conclusion

In this chapter, we introduced our architecture VFed-IDS which aims to provide a defensive mechanism against cyber-threats with the privacy-preserving in connected vehicles by applying the Federated Learning technique with the powerful features of the Blockchain technology. Our work made it possible for the connected vehicles to participate in building a robust IDS against diverse attacks which leads the way to have more autonomous and intelligent vehicles. The privacy-preserving process is established without revealing any private dataset of the participating vehicles. Extensive simulations were carried out using the NSL-KDD dataset to assess the performance of the proposed VFed-IDS framework. The outcomes demonstrated that VFed-IDS outperformed other existing models in terms of both effectiveness and efficiency for the IoV. The framework exhibited a high accuracy rate of 99% in detecting malicious nodes.

# CHAPITRE 6

# CONCLUSION AND PERSPECTIVES

The research work in this thesis concerns the security of IoV. It is about establishing secure, scalable and trustworthy communications between participating vehicles and infrastructure's components while preserving privacy. This thesis is organized into five chapters :

In the first chapter, we overviewed IoV, discussed their characteristics, applications, architecture components, communications types, the presentation of SDN and its integration in these networks. We discussed its security and privacy concerns.

In Chapter 2, we elucidated the trust management mechanism within the context of the Internet of Vehicles (IoV). Our presentation encompassed the latest and most sophisticated schemes developed specifically for IoV. We conducted a thorough examination of existing surveys pertaining to security in vehicular networks. Additionally, we offered a comprehensive overview of the fundamental pillars of trust, including properties, metrics employed, and modules incorporated in IoV trust management. Subsequently, we delved into the intricate challenges posed by security and trust in Vehicular networks, presenting a dual classification based on both fundamental characteristics and the technological underpinnings of the most relevant trust management approaches for connected vehicles. A qualitative comparison was then provided, utilizing a set of criteria to assess the effectiveness of these approaches.The chapter concluded by shedding light on potential open issues and future perspectives in the realm of trust management for connected vehicles.

In Chapter 3, we introduced a hierarchical architecture designed to enhance the security of software-defined vehicular networks. Additionally, we proposed a security model for predicting and detecting Distributed Denial of Service (DDoS) attacks, leveraging behavioral analysis of nodes through a Markov stochastic process. Our contribution outlined three primary layers : the data layer, Software-Defined Networking (SDN), and Cloud. We categorized participating vehicles based on a detailed range policy and identified five distinct states : heavily malicious, lightly malicious, heavily suspicious, lightly suspicious, and authentic vehicles. The state of a vehicle at time t+1 was contingent upon its state at time t. The results from conducted simulations demonstrated the proactive and reliable mitigation of DDoS attacks by our model.

In chapter 4, we introduced a decentralized trust model using the Blockchain technology, smart contracts to establish a robust trust management system for connected vehicles where we developed four smart contracts. The first managed the rating values of participating vehicles. The second was responsible for managing the pseudo-identities of vehicles within the network. The third controlled the access management of entities in the network. The last smart contract managed the participation of the vehicles in the network by adding or removing the pseudo-id of vehicles with rating value greater or lower than a prefixed threshold respectively. Thus, only authenticated and highly trusted vehicles communicated with other entities of the vehicular architecture.

In chapter 5, we introduced another security and privacy-preserving scheme by combining the Federated Learning with the power of the Blockchain. In this contribution, we presented a new intrusion detection system, where the training phase was not only integrated in a central entity but in the connected

vehicles. The Federated Learning process started by training local models in the authenticated vehicles. Then, the SDNC managed the aggregated local trained models to pick the best model which was broadcasted then to all the nodes in the network. Integrating the Blockchain and smart contract provided a deterministic, secured and updated platform to manage the models by hashing the exchanged models' updates between the connected vehicles and the SDNC. Our contribution enhanced effectively the autonomous behavior of the connected vehicles and improved the privacy of drivers. Our thesis focuses on augmenting the security of connected vehicles, specifically by developing models to fortify the communications between various network components within the Internet of Vehicles (IoV). Despite these efforts, several unresolved issues warrant further investigation.
In this section, we delve into key challenges and propose potential avenues for future research aimed at bolstering security and preserving privacy in IoV. We highlight three promising directions : Federated Learning-based solutions, Clustering approaches, and the integration of emerging technologies, along with an exploration of auction-based solutions. These avenues represent potential strategies to address the existing challenges and contribute to the ongoing evolution of secure communication within the IoV framework.

In this thesis, we introduced a lightweight prediction and detection model for mitigating Distributed Denial of Service (DDoS) attacks in the context of Internet of Vehicles (IoV) and conducted extensive simulations to evaluate its performance. However, it is important to note that the model's effectiveness diminishes when confronted with the need for scalability. Our primary aim with this contribution is to develop a model that enhances scalability.Vehicular networks are characterized by their large-scale nature, particularly in densely populated urban areas such as big cities, highways, and downtown locations. Consequently, a substantial volume of data is generated and processed rapidly by each network node. Machine Learning emerges as one of the most rapidly evolving technological tools, offering a practical means to efficiently process this vast amount of data within minimal time. This approach allows the system to autonomously learn and enhance its security based on past data processing experiences.

Incorporating Artificial Intelligence-powered techniques into trust management within the Internet of Vehicles (IoV) context enhances network efficiency. Federated Learning, as a decentralized Machine Learning method, addresses concerns related to centralized training. It allows all network participants to collaborate in the creation of a global model without the need to share their data. In the IoV setting, participant nodes often assume distinct roles and responsibilities. Consequently, Federated Learning contributes to the development of resilient trust algorithms and models that leverage a variety of parameters and metrics through distributed intelligent approaches.

In the context of the Internet of Vehicles (IoV), the cross-domain protocol plays a crucial role in authenticating connected vehicles as they move across different domains. This protocol is essential due to the frequent need for vehicles to travel across various domains. Currently, the Public Key Infrastructure (PKI) system is commonly employed to address identity authentication and security trust issues faced by connected vehicles. However, several challenging issues have been identified with the PKI system, including the overly centralized authority of Certification Authorities (CAs), regular cross-domain access to certificate interactions, high certificate management costs due to the substantial authentication volume, complex authentication paths across domains, potential privacy leakage, and network overburdening. As part of our future work, we aim to develop a Blockchain-based solution to address these challenges. Our proposed solution involves creating a lightweight PKI identity management system and authentication architecture using smart contracts. This approach is designed to alleviate the burdens associated with CAs directly controlling the life cycle of digital certificates, offering a more efficient and secure alternative for managing identity authentication in the IoV environment.

Our upcoming contributions focus on the integration of the clustering paradigm with decentralized trust management, aiming to enhance the reliability of systems, particularly in the context of incorporating emerging decentralized technologies such as Software-Defined Networking (SDN) or Blockchain within the Internet of Vehicles (IoV). These technologies are anticipated to enhance both the performance and coordination among different entities, namely Cluster Heads (CH) and Cluster Members (CM) in the IoV environment.To achieve this, we plan to incorporate a trust metric into the clustering formation and the selection of the cluster head. The node with the highest trust value will be elected as the Cluster Head, adding an additional layer of security and reliability to the clustering process. Furthermore, we are exploring the development of a Cluster Head backup system to ensure the stability of clusters in the IoV, mitigating potential disruptions and enhancing the overall robustness of the system.

Vehicular networks, known for their high scalability, face notable challenges in terms of energy effi-

ciency, particularly given the substantial data exchanged among network components. The deployment of new mechanisms or technologies in the Internet of Vehicles (IoV) often results in increased communication overhead and complexity, posing difficulties in meeting real-time application requirements. Recognizing these challenges, our focus is on achieving a favorable trade-off between the integration of emerging technologies and energy efficiency. Our approach emphasizes the implementation of lightweight solutions to reduce overall system energy consumption. By prioritizing efficiency, we aim to strike a balance that allows for the seamless integration of emerging technologies within vehicular networks while mitigating the associated challenges related to energy consumption. This pursuit aligns with the goal of optimizing the performance of IoV systems without compromising on their energy efficiency.

Finally, we are also investigating the distribution of resource mechanisms in the IoV because we have noticed that the crooked distribution of resources and incentives on IoV has paved an easy route for attackers to take the repercussions of DDoS attacks to a challenging level. As a future perspective, we aim to combine the auction concept with the Blockchain in IoV, where we will have a central entity responsible for providing nodes with the necessary resources after submitting their bid values. The service provider will allocate the resource to the vehicle with the best bid value each auction round. However, attacking vehicles will try to falsify the bid values of other vehicles so that they win the auction rounds each time and take all the resource units selfishly. We aim to develop a robust cyber-threat defensive framework based on the Bayesian game theory, where the system can predict malicious nodes. We also aim to develop a reputation system where the vehicles that utilize most of the demanded/claimed units are considered honest nodes, and their reputation scores will be increased.

# ANNEX : Résumé en Français

Malgré les avancées technologiques et les initiatives politiques visant à renforcer la sécurité routière, de nombreux systèmes de transport dans le monde continuent de faire face à des problèmes graves en termes de sécurité et d'efficacité. Selon l'Organisation Mondiale de la Santé (OMS) [1], on enregistre chaque année 1,35 million de décès liés aux accidents de la route dans le monde. Cela signifie qu'environ 3 700 personnes perdent la vie chaque jour en raison d'accidents impliquant des voitures, des bus, des motos, des vélos, des camions ou des piétons. Plus de la moitié des victimes sont des piétons, des motocyclistes ou des cyclistes. Les blessures résultant d'accidents routiers sont estimées comme étant la huitième cause de décès dans le monde, toutes tranches d'âge confondues, et la principale cause de décès chez les enfants et les jeunes âgés de 5 à 29 ans.

Afin de surmonter ces problèmes, les Systèmes de Transport Intelligents (STI) sont développés pour fournir aux véhicules et aux infrastructures de transport des capacités de communication sécurisées, robustes et fiables. Ces systèmes visent à offrir des avantages tels que des routes plus sûres (moins d'accidents), une meilleure efficacité (moins de temps passé sur la route et moins de pollution), un confort accru pour les passagers (divertissement multimédia, infodivertissement, etc.) et une sécurité élevée (modèles intelligents renforçant la sécurité, réduisant les attaques) en matière de mobilité. La combinaison des capacités de communication avec les capacités de détection et de perception fournies par les capteurs intégrés aux véhicules ouvre la voie au développement de nombreux services dans le domaine des STI.

Les STI offrent une large gamme de services conçus pour atteindre ces objectifs, tels que le service de Prévention des Collisions Coopératives (CCA), qui permet aux véhicules d'éviter les accidents en échangeant des informations de mobilité. Un autre service est la Perception Coopérative (vue d'ensemble), qui permet à chaque véhicule de créer une vision globale de son environnement en combinant les informations locales des véhicules voisins pour prendre des décisions efficaces, comme la planification de trajectoires futures. Un autre service présenté dans les STI est la Conduite en Peloton (Platooning), qui vise à regrouper les véhicules en convois de plusieurs véhicules rapprochés pour économiser le carburant, prévenir les accidents et optimiser l'utilisation des routes.

Les réseaux véhiculaires jouent un rôle crucial dans la résolution des problèmes liés à la circulation dans les zones urbaines. La combinaison du cloud computing, de l'informatique de pointe, du Big Data et de l'Internet des objets (IoT) a conduit à l'évolution des réseaux de véhicules, donnant naissance au paradigme de l'Internet des véhicules (IoV) [1]. L'IoV suscite un vif intérêt à la fois dans le monde universitaire et l'industrie. En conséquence, la prochaine génération de véhicules sera connectée et équipée d'une ou plusieurs interfaces, permettant la communication avec d'autres éléments du système de transport intelligent, tels que d'autres véhicules connectés, des piétons et des infrastructures telles que les unités embarquées (OBU), les unités routières (RSU), les stations de base (BS) et le Cloud. L'ensemble de ces entités et leurs interactions forment un réseau de communication appelé réseau véhiculaire, un élément crucial pour le bon fonctionnement de l'IoV. L'objectif de ces réseaux est d'assurer la connectivité réseau nécessaire avec les performances requises par l'écosystème de l'IoV.

Les véhicules connectés, grâce aux communications Vehicle-to-Everything (V2X), contribuent à des flux de trafic plus sûrs et efficaces, soutenant la mobilité et le transport routier de nouvelle génération. Les communications V2X englobent une variété de communications dans lesquelles les véhicules connectés

utilisent des médias sans fil pour échanger des informations avec d'autres véhicules, les infrastructures environnantes, les capteurs embarqués, les appareils personnels et les serveurs de cloud computing. Les systèmes d'application basés sur le V2X incluent généralement des applications critiques pour la sécurité, telles que la gestion de la congestion routière, la prévention des accidents et les notifications de collisions. Ils incluent également des applications non liées à la sécurité, comme la navigation et le divertissement. La communication V2X, combinée aux capacités des capteurs intégrés aux véhicules, améliore la gestion du trafic et la sécurité routière en diffusant des avertissements de collision, des notifications de freinage d'urgence, des alertes de danger, des informations sur les obstacles et des notifications d'embouteillages. En raison de la nature critique de ces applications, il est essentiel que les informations échangées soient sécurisées et fiables. Cependant, ces messages sont vulnérables aux attaques, où des véhicules malveillants peuvent simuler des messages de sécurité et retarder leur transmission, entraînant ainsi de graves accidents et des pertes de vies humaines.

Tesla est réputé pour ses mesures de cybersécurité, en particulier son système de défi sophistiqué qui protège ses voitures contre les méthodes traditionnelles d'attaque à distance. Cependant, récemment, un chercheur a découvert une attaque sophistiquée utilisant la technique de relais, qui permettrait à une personne ayant un accès physique à une Tesla Model Y de la déverrouiller et de la voler en quelques secondes.

En raison de leur importance stratégique dans la facilitation des communications au sein de l'Internet des Véhicules (IoV), les réseaux de véhicules sont devenus très populaires ces dernières années. L'augmentation rapide du nombre de véhicules connectés sur les routes a également conduit au développement de réseaux de véhicules hétérogènes, à grande échelle et très dynamiques. On estime qu'il y aura plus de 500 millions de voitures connectées sur les routes d'ici 2025. Cependant, ces réseaux rencontrent des défis pour répondre à des exigences strictes telles que la faible latence, la mobilité élevée, la sécurité optimale et la connectivité massive du réseau 5G/6G. En conséquence, la nature hautement mobile et décentralisée de ces réseaux, ainsi que leur infrastructure ouverte, les rendent vulnérables aux attaques internes et externes. Au fil des décennies, des chercheurs universitaires et de l'industrie ont proposé des solutions de sécurité basées sur la cryptographie, mais ces approches se sont principalement révélées efficaces contre les attaques externes, où les attaquants ne sont pas des nœuds du réseau autorisés.

Tesla, en particulier, est reconnu pour ses mesures de cybersécurité, notamment un système de défi sophistiqué qui protège ses voitures contre les attaques traditionnelles visant à déverrouiller les véhicules à distance. Cependant, étant donné que les voitures de Tesla sont bien plus technologiques que celles des autres constructeurs, leur surface d'attaque est plus grande, ce qui crée des opportunités pour les attaquants de trouver des vulnérabilités. En 2017, un groupe de chercheurs chinois en sécurité a réussi à pirater une Tesla Model X à deux reprises, effectuant des actions telles que le freinage à distance, l'ouverture et la fermeture des portes et du coffre, tout en faisant clignoter les lumières au rythme de la musique diffusée depuis la radio de la voiture, un effet surnommé "le spectacle de Noël non autorisé".

En 2022, Josep Pi Rodriguez, chercheur et consultant principal en sécurité pour IOActive, a découvert une attaque sophistiquée utilisant la technique de relais. Cette attaque permettait à toute personne ayant un accès physique à une Tesla Model Y de la déverrouiller et de la voler en quelques secondes. La vulnérabilité découverte implique une attaque par relais NFC qui nécessite la collaboration de deux voleurs. Un voleur doit se trouver à proximité de la voiture, tandis que l'autre doit être à proximité du propriétaire de la voiture, qui possède soit une carte-clé NFC, soit une clé virtuelle Tesla sur son téléphone portable dans sa poche ou son sac à main. Les cartes-clés NFC permettent aux propriétaires de Tesla de déverrouiller leur véhicule et de démarrer le moteur en plaçant la carte contre un lecteur NFC intégré dans la carrosserie du côté conducteur de la voiture. Les propriétaires peuvent également utiliser un porte-clés ou une clé virtuelle sur leur téléphone portable pour déverrouiller leur voiture, mais le manuel de la voiture recommande toujours d'avoir sur soi la carte-clé NFC comme sauvegarde au cas où ils perdraient le porte-clés ou le téléphone, ou si la batterie de leur téléphone venait à s'épuiser. Le piratage complexe impliquait l'envoi de logiciels malveillants via le navigateur Web de la voiture dans le cadre d'une série d'exploits informatiques détournés. Cela permettait aux pirates de contrôler la voiture à distance via Wi-Fi et une connexion cellulaire.

Par exemple, Nissan a dû retirer son application pour la voiture électrique Leaf après qu'elle se soit révélée vulnérable au piratage. De même, Fiat Chrysler Automobiles a rappelé environ 1,4 million de véhicules en raison de la capacité des pirates informatiques à accéder électroniquement aux voitures et à gérer les fonctions de freinage et d'accélération grâce à une faille de sécurité dans le logiciel.

Comme indiqué précédemment, les réseaux de véhicules sont très vulnérables aux attaques en raison de leur grande mobilité et de leur dynamisme, où les nœuds malveillants peuvent modifier les messages critiques pour la sécurité et introduire des retards extrêmes dans la communication. Cela peut provoquer des accidents de la route et entraîner la perte de vies humaines précieuses. Les réseaux de véhicules sont de plus en plus ouverts, et leur accès illimité les rend plus exposés aux attaques. Il est essentiel de prouver et d'améliorer la sécurité des services du framework IoV avancé. Ces attaques peuvent être classées comme internes, externes, actives ou passives. De plus, l'anxiété concernant l'utilisation abusive de données privées est également ressentie par les utilisateurs du réseau. Par conséquent, plusieurs nouveaux systèmes de sécurité ont été proposés pour détecter et contrer ces attaques, ce qui constitue un domaine de recherche majeur.

Le développement de modèles de sécurité robustes pour les véhicules permet d'éviter l'échange de messages modifiés et critiques pour la sécurité. Ces modèles permettent de révoquer les véhicules malveillants qui diffusent de telles informations falsifiées en intégrant des modèles de sécurité intelligents basés sur des approches telles que les modèles stochastiques, les technologies émergentes telles que la Blockchain, les réseaux définis par logiciel (SDN), ainsi que des techniques puissantes de machine learning (ML) auxquelles ils peuvent s'adapter. Ces modèles doivent être capables de comprendre la nature dynamique des réseaux de véhicules, de détecter les anomalies, de protéger la vie privée des utilisateurs, et de se défendre de manière proactive contre un large éventail de menaces. Tout ceci garantit la sécurité des véhicules connectés, de leurs occupants, et la confiance dans la nature des expéditeurs ainsi que des informations échangées.

Il est impératif qu'un véhicule malveillant soit identifié et éliminé avant qu'il n'ait la moindre opportunité de causer des dommages au réseau. Par exemple, imaginez à quel point il serait dommageable qu'un véhicule malveillant modifie un message d'avertissement d'évitement de collision, mettant en garde un autre véhicule d'un accident imminent sur son itinéraire, ce qui pourrait entraîner des accidents mortels et la perte de vies humaines.

Les mécanismes de sécurité traditionnels ne sont pas toujours adaptés pour faire face aux caractéristiques uniques des réseaux de véhicules dans leur ensemble, afin de fournir une défense significative dans des scénarios spécifiques à l'Internet des véhicules (IoV). Les systèmes cryptographiques ont été largement déployés pour atténuer les comportements malveillants des véhicules adverses. Cependant, d'autres solutions centralisées sont nécessaires pour évaluer la crédibilité des véhicules authentifiés, et les solutions existantes sont principalement conçues pour traiter les attaquants extérieurs, ne suffisant pas lorsque le véhicule malveillant est un membre honnête du réseau. Les exigences de sécurité traditionnelles, telles que la confidentialité, l'intégrité, l'authentification et la disponibilité, doivent toujours être satisfaites.

De plus, des étapes supplémentaires peuvent être nécessaires en fonction des besoins spécifiques de l'IoV dans un scénario donné, comme l'audit du suivi et de la fiabilité des informations. L'intégration de modèles stochastiques, tels que les chaînes de Markov, peut permettre de capturer la nature dynamique des réseaux de véhicules et d'aider à prendre des décisions en se basant sur l'état actuel et les probabilités de transition. Ces modèles peuvent prédire les futurs états de sécurité des véhicules connectés en se basant sur des données historiques. En analysant les transitions et les événements passés, ils peuvent fournir des informations sur les vulnérabilités ou les menaces potentielles qui pourraient survenir dans un avenir proche, permettant ainsi de prendre des mesures de sécurité proactives.

Dans cette optique, la combinaison de la technologie SDN avec les réseaux de véhicules pour unifier leurs plans de contrôle permet aux réseaux de véhicules d'utiliser plusieurs technologies d'accès. Cela leur permet de tirer parti des capacités des différents réseaux d'accès et d'offrir une flexibilité dans leur contrôle et leur gestion. Cette flexibilité est nécessaire pour gérer efficacement les ressources réseau disponibles et fournir des services de communication adaptés aux exigences de sécurité des réseaux de véhicules.

La notion de confiance a récemment été introduite pour faire face aux attaques internes au sein des réseaux automobiles. Par conséquent, le développement de modèles de sécurité des véhicules basés sur la confiance vise à prévenir l'échange de messages malveillants provenant de véhicules attaquants, et contribue également à révoquer leur accès. La gestion de la confiance vise à évaluer les données et les entités échangées en attribuant des valeurs de confiance pour garantir la sécurité routière. L'intégration de la Blockchain dans le processus de gestion de la confiance fournit une plate-forme décentralisée avec un registre mis à jour des valeurs de confiance disponibles et accessibles pour les nœuds participants. Ainsi, les véhicules et les unités routières (RSU) peuvent demander la valeur de confiance de n'importe quel autre nœud.

Le développement d'un système de détection d'intrusion basé sur l'apprentissage fédéré et la blockchain dans les réseaux de véhicules offre une approche puissante et globale de la sécurité et de la confidentialité. Il combine l'apprentissage décentralisé, la préservation de la confidentialité, la technologie du registre inviolable et les mécanismes de défense collaboratifs pour créer un système IDS sécurisé et adaptable

capable de protéger efficacement les réseaux de véhicules contre diverses menaces de sécurité tout en préservant la confidentialité des participants au réseau. Cette approche est cruciale pour garantir la sûreté, la sécurité et la fiabilité des systèmes de communication des véhicules.

À la lumière de ce qui précède, la recherche vise à explorer la possibilité de concevoir des modèles intelligents pour sécuriser les communications entre les véhicules connectés et s'adapter à l'évolutivité du réseau. Nos modèles de sécurité assurent la confidentialité conditionnelle des conducteurs et améliorent le comportement autonome des véhicules connectés. Dans le contexte de l'Internet des véhicules (IoV), les informations transmises sont distribuées dans un environnement d'accès ouvert, ce qui rend la sécurité et la confidentialité parmi les problèmes les plus critiques liés aux réseaux de véhicules. Par conséquent, tout système basé sur l'IoV doit répondre aux exigences de services de sécurité et de confidentialité pour assurer l'efficacité et la fiabilité du système. Il est essentiel de garantir que les messages échangés ne soient ni insérés ni modifiés par des attaquants, qu'ils soient internes ou externes, malveillants ou rationnels, locaux ou étendus, actifs ou passifs. Toute application impliquée peut représenter une menace sérieuse pour la sécurité des conducteurs et des passagers. Selon l'Organisation mondiale de la santé, chaque année, plus de 1,35 million de personnes trouvent la mort sur les routes. Par conséquent, l'authentification et la confiance dans l'échange étendu de données sont des exigences cruciales dans le domaine de l'IoV.

La confidentialité et la sécurité des informations échangées dans les réseaux de véhicules sont des préoccupations majeures. Les autorités de confiance (TA) jouent un rôle crucial dans la gestion de l'accès aux informations sensibles et privées sur les véhicules. Leur mission principale est de préserver la vie privée des conducteurs en empêchant l'accès non autorisé à ces données. Cela signifie que seules les TA ont la capacité d'accéder à ces informations sensibles.

Les TA sont chargées de plusieurs tâches essentielles, notamment : Générer et gérer les clés privées et les paramètres de sécurité pour les véhicules et les unités routières (RSU) participants. Fournir des pseudo-identités pour les véhicules immatriculés, préservant ainsi la vie privée des utilisateurs tout en permettant de retracer les activités malveillantes. Surveiller le réseau pour détecter les faux messages diffusés par des nœuds malveillants. L'utilisation de pseudo-identités est un mécanisme important pour préserver la confidentialité tout en permettant la détection des activités malveillantes. Les RSU jouent également un rôle dans l'analyse des messages reçus pour prévenir les attaques de fausses informations. En résumé, la combinaison de TA, de pseudo-identités et de surveillance du réseau contribue à préserver la confidentialité des données tout en garantissant l'authenticité et la sécurité des messages échangés dans les réseaux de véhicules. La sécurité des réseaux de véhicules est un défi crucial, et l'infrastructure à clé publique (PKI) joue un rôle essentiel pour garantir l'authenticité et la sécurité des communications. Cependant, les PKI traditionnelles ont des limites, notamment dans la détection des attaquants internes, car ces attaquants ont généralement des informations d'identification vérifiées.

Les approches basées sur la confiance émergent comme une solution prometteuse pour renforcer la sécurité dans les réseaux de véhicules. Ces approches permettent à chaque nœud de noter la confiance qu'il accorde à d'autres nœuds avec lesquels il communique. La gestion de la confiance est cruciale pour diffuser des informations fiables, prévenir les faux messages, détecter les comportements égoïstes et malveillants, et atténuer leurs activités nuisibles. Les modèles de confiance peuvent être implémentés dans les unités routières (RSU) et les véhicules pour évaluer la fiabilité, l'exactitude et l'authenticité des messages échangés.Cela montre que les chercheurs s'efforcent de mettre au point des mécanismes de sécurité plus avancés pour les réseaux de véhicules, notamment en s'appuyant sur des concepts tels que la confiance pour renforcer la sécurité et la fiabilité des communications.

Dans notre troisième contribution, nous présentons une architecture SDVN hiérarchique qui comprend trois couches distinctes : la Couche Données, la Couche SDN et la Couche Cloud.

La Couche Données comprend des nœuds statiques et dynamiques responsables de la collecte en temps réel de données, qui sont ensuite transmises à la Couche SDN. Ces nœuds peuvent être des véhicules connectés, des unités routières (RSU) ou des stations de base (BS). Les véhicules dans le SDVN sont dotés de deux interfaces réseau ou plus. Une interface leur permet d'accéder au réseau RSU via la communication dédiée à courte portée (DSRC), tandis qu'une autre leur permet d'accéder au réseau cellulaire (LTE/5G).

La Couche SDN est subdivisée en deux niveaux de contrôle : le niveau de contrôle 1 comprend les contrôleurs locaux, à savoir le contrôleur d'unités routières (RSUC) et le contrôleur de stations de base (BSC). Le niveau de contrôle 2 est composé du contrôleur principal de l'architecture, le contrôleur SDN (SDNC). La Couche SDN traite les données soumises et les analyse. Elle répond aux besoins avancés des réseaux de véhicules tels que l'évolutivité, la latence, l'hétérogénéité, la mobilité élevée, la faible latence de communication et le débit élevé grâce à la mise en œuvre des fonctionnalités SDN.

La couche Cloud est chargée de gérer de vastes quantités de données pour atténuer les attaques DDoS dans les architectures SDVN. Nous proposons trois sous-modèles pour cela, à savoir le modèle collecteur,

le modèle de prédiction et de détection, ainsi que le modèle de réaction.

Notre modèle de sécurité est constitué de trois sous-modèles visant à sécuriser l'architecture SDVN contre les attaques DDoS :

Modèle collecteur : Les stations de base (BS) et les unités routières (RSU) de la couche de données assurent la surveillance des véhicules connectés. Ils collectent toutes les données échangées avec les véhicules dans le réseau, que ce soit par le biais des communications DSRC ou 5G/LTE. Dans notre travail, le modèle collecteur utilise le protocole SFlow pour rassembler toutes les données des utilisateurs externes vers le SDNC, en passant par les serveurs cloud, ainsi que les données des véhicules de la couche de données jusqu'au premier niveau de contrôle du SDN.

Modèle de prédiction et de détection : Dans ce module, nous analysons et classons les données collectées des deux sens, attribuant un statut à chaque session. Nous définissons cinq statuts : Authentique (Auth), Légèrement suspect (LS), Fortement suspect (HS), Légèrement malveillant (LM) et Fortement malveillant (HM). L'authenticité d'une session est déterminée en fonction du nombre de journaux enregistrés (LOG.size), qui doit être inférieur à 25% de la taille de la mémoire de la table de flux du commutateur, d'où la fixation de th1 à 0,25. Le statut LS est attribué lorsque LOG.size est supérieur à th1 mais inférieur à 45% de la taille de la mémoire de la table de flux de commutation, et th2 est donc fixé à 0,45. Enfin, le statut HS est déterminé en cas de comportement malveillant, lorsque LOG.size dépasse th2, ce qui indique une possible attaque.

Modèle de réaction : Dans ce module, nous avons mis en place un algorithme de réaction pour contrer les attaques détectées par le modèle de prédiction et de détection en fonction de l'état de chaque session. Les sessions honnêtes, qui sont des nœuds authentiques du réseau, se voient attribuer davantage de bande passante, ce qui implique l'application d'un mécanisme de récompense. En revanche, les sessions malhonnêtes, c'est-à-dire les nœuds fortement malveillants, sont directement bloquées. En ce qui concerne les sessions suspectes, à la fois légèrement et fortement suspectes, elles sont considérées comme des sessions malveillantes, mais aucune action immédiate n'est entreprise pendant un créneau horaire spécifique ($T_{slot}$). Cependant, une enquête ou une observation plus approfondie est nécessaire. Un nœud suspect peut changer son statut pour devenir honnête et autorisé, ou malhonnête et bloqué, en fonction de son comportement, tel que déterminé par l'algorithme de réaction.

Notre modèle de sécurité stochastique a pour objectif de détecter les attaques DDoS en se basant sur le comportement des appareils, puis de prédire leur état futur à l'aide d'un modèle de chaîne de Markov et d'une matrice de probabilité de transition stochastique. Dans ce travail, nous utilisons un processus stochastique de Markov pour analyser le comportement de chaque appareil. En fonction du journal des événements, nous définissons différentes plages de comportement en utilisant divers seuils pour identifier le comportement de chaque appareil, qu'il s'agisse d'utilisateurs externes ou de véhicules connectés du plan de données.

Le but de cette contribution est de réduire les attaques DDoS qui surviennent lorsque le système est submergé. Il existe deux types d'attaques de sécurité : celles qui sont légèrement malveillantes et celles qui sont fortement malveillantes. Les attaques légèrement malveillantes peuvent se produire par accident en raison de mauvaises manipulations de l'appareil, mais de nombreuses attaques sont le fait d'appareils malveillants. Notre modèle stochastique vise à identifier l'état de l'appareil en se basant sur le nombre d'activités de lecture dans le journal. Nous utilisons un mécanisme de plages de comportement de session. Nous classifions ces sessions en cinq catégories : Authentique, Légèrement Suspect, Fortement Suspect, Légèrement Malicieux et Fortement Malicieux, en utilisant quatre seuils de valeurs fixes : th1, th2, th3 et th4. Nous pouvons ensuite identifier l'état de chaque session. Par exemple, une session avec l'état Fortement Suspect au début d'un Time Slot $T_{slot}$ peut passer à l'état Fortement Malicieux si le nombre d'activités signalées dépasse le seuil th4. Dans ce chapitre, nous présentons sept états comme suit : - État authentique (Auth) : la taille du journal de l'appareil est inférieure à th1. - État légèrement suspect (LS) : la taille du journal de l'appareil est comprise entre th1 et th2. - État fortement suspect (HS) : la taille du journal de l'appareil est entre th2 et th3. - État légèrement malveillant (LM) : la taille du journal de l'appareil est comprise entre th3 et th4. - État fortement malveillant (HM) : la taille du journal de l'appareil est supérieure à th4. - État de blocage : une fois l'attaque survenue. - État d'observation (Observ) : la taille du journal de l'appareil est comprise entre th2 et th4. Cela signifie que seuls les nœuds classifiés comme authentiques seront directement autorisés, tandis que tous les autres nœuds seront observés pendant un créneau horaire. Cette contribution a présenté une architecture SDVN hiérarchique conçue pour être sécurisée contre les attaques DDoS, en utilisant un modèle mathématique de Markov. Notre architecture comprend trois couches : la couche Data, la couche SDN et la couche Cloud. Le modèle de sécurité se compose de trois sous-modèles : le modèle collecteur, le modèle de prédiction et de détection, et le modèle de réaction. Dans ce travail, nous avons approfondi le modèle de Markov stochastique de prédiction et de détection. Nous l'avons évalué à l'aide de MATLAB pour

analyser le comportement des nœuds dans le réseau et prédire leurs états futurs en fonction de leurs états actuels. Enfin, nous avons procédé à l'évaluation de notre solution, démontrant qu'elle constitue une solution légère avec un taux de détection élevé et une atténuation plus rapide grâce à la probabilité et aux formules analytiques du modèle de chaîne de Markov à temps discret.

Avec l'avènement des véhicules connectés, l'industrie automobile est confrontée à un besoin essentiel de systèmes de gestion de confiance robustes. La croissance de la connectivité et de l'automatisation des véhicules modernes les expose à diverses menaces de sécurité, ce qui nécessite des solutions innovantes pour garantir la sécurité, la confidentialité et la fiabilité. Dans ce contexte, divers mécanismes basés sur la confiance ont été introduits pour sécuriser les véhicules connectés et favoriser les systèmes de transport intelligents (STI) sécurisés. Cependant, ces solutions présentent des limites, notamment un manque de flexibilité, de transparence et d'efficacité. De plus, elles reposent souvent sur des entités de confiance centralisées pour l'échange de certificats et de clés de sécurité, introduisant ainsi un risque de point de défaillance unique et de fragilité du système.

Afin de relever ces défis, nous présentons un cadre de gestion de la confiance entièrement décentralisé basé sur la technologie de la blockchain. Ce cadre utilise plusieurs contrats intelligents pour établir la confiance et garantir la sécurité au sein des futurs réseaux de véhicules définis par logiciel (SDVN) de manière distribuée, transparente, sécurisée, inviolable et fiable. Notre système a été implémenté, testé et déployé sur le réseau Ethereum. Les résultats expérimentaux confirment que notre solution offre adaptabilité, sécurité, efficacité et rentabilité, ce qui en fait une avancée prometteuse pour le développement de nouveaux systèmes de gestion de la confiance décentralisée dans le domaine des STI. Les principales contributions du quatrième chapitre sont les suivantes : Nous avons conçu un nouveau cadre basé sur la blockchain, utilisant plusieurs contrats intelligents pour établir la confiance et garantir la sécurité au sein des futurs réseaux de véhicules définis par logiciel (SDVN). Ce cadre fonctionne de manière entièrement distribuée, transparente, sécurisée, inviolable et fiable. Nous avons proposé un modèle de gestion des pseudonymes basé sur la blockchain pour sécuriser les communications entre les véhicules, les unités de bord de route (RSU) et les unités de contrôle de route (RSUC). L'objectif de ce modèle est de préserver l'anonymat et la vie privée, tout en répondant aux exigences de sécurité des réseaux de véhicules connectés. Nous avons présenté un Trust Smart Contract (TSC) pour établir et gérer la confiance au sein du réseau de véhicules, améliorant ainsi la sécurité, la transparence et la fiabilité. Nous avons également proposé un Revoke Smart Contract (RSC) chargé de gérer la révocation de la confiance des véhicules engagés dans des activités malveillantes ou compromis. Le RSC bannit officiellement les véhicules malveillants du réseau en révoquant leurs certificats, garantissant ainsi que seuls les rapports d'événements légitimes sont diffusés sur le réseau. Enfin, nous avons introduit un contrat intelligent de contrôle d'accès (ACSC) pour réguler les politiques de contrôle d'accès au sein du réseau automobile.

Les réseaux de véhicules sont confrontés à des défis majeurs pour répondre à leurs exigences en matière de faible latence, mobilité élevée, connectivité massive (6G) et sécurité maximale. Pour déployer un système de détection d'intrusion robuste dans l'Internet des Véhicules (IoV), des progrès significatifs sont nécessaires. Le cinquième chapitre de cette thèse présente VFed-IDS, une architecture décentralisée, sécurisée, flexible, évolutive et robuste basée sur la blockchain et l'apprentissage fédéré. Cette architecture se compose de trois couches principales : la couche centrale, la couche locale et la couche Blockchain. La couche centrale comprend le contrôleur SDN qui entraîne et agrège le modèle global, tandis que la couche locale comprend les véhicules qui entraînent des modèles locaux en utilisant leurs données locales privées. La couche Blockchain gère le cryptage des transactions entre les couches centrale et locale, et intègre notre Smart Contract VFed-SC, qui gère la liste des véhicules authentifiés et collaborateurs dans le processus d'apprentissage fédéré. Les résultats de simulation démontrent que VFed-IDS offre un taux de précision élevé et améliore le comportement autonome des véhicules connectés face aux cybermenaces.

Les travaux de recherche de cette thèse se concentrent sur la sécurité des réseaux véhiculaires, avec pour objectif d'établir des communications sécurisées, évolutives et fiables entre les véhicules participants et les composants de l'infrastructure, tout en préservant la confidentialité. Cette thèse est organisée en cinq chapitres, chacun explorant divers aspects de la sécurité des réseaux véhiculaires et proposant des solutions innovantes pour répondre à ces défis.

Dans le premier chapitre, nous avons introduit les réseaux de véhicules en explorant leurs caractéristiques, applications, composants d'architecture, types de communication, ainsi que l'introduction du Software-Defined Networking (SDN) et de son intégration dans ces réseaux. Nous avons également abordé les enjeux de sécurité et de confidentialité associés à ces réseaux.

Dans le chapitre 2, nous avons exploré le mécanisme de gestion de la confiance au sein des réseaux de véhicules. Nous avons présenté les derniers schémas élaborés dans le contexte de l'Internet des Véhicules (IoV) et examiné les enquêtes existantes en matière de sécurité dans les réseaux de véhicules. Nous avons également proposé un résumé global des principaux éléments constitutifs de la confiance, y compris leurs propriétés, les métriques utilisées, et les modules associés. En outre, nous avons abordé les défis complexes relatifs à la sécurité et à la confiance dans les réseaux de véhicules. Nous avons proposé une classification, non seulement de base, mais également basée sur les technologies utilisées, des approches les plus pertinentes pour la gestion de la confiance des véhicules connectés. Nous avons ensuite effectué une comparaison qualitative en nous basant sur divers critères. Le chapitre s'est conclu en mettant en lumière certaines questions en suspens et des perspectives ouvertes pour de futures recherches.

Dans le chapitre 3, nous avons présenté une architecture hiérarchique pour la sécurisation des réseaux de véhicules définis par logiciel (SDVN) et un modèle de sécurité visant à prédire et détecter les attaques DDoS. Notre approche repose sur l'analyse comportementale des nœuds, réalisée au moyen d'un processus stochastique de Markov. Au sein de cette contribution, nous avons introduit trois couches principales : la couche de données, le SDN et le Cloud. Les véhicules participants ont été classés en fonction d'une politique de gamme détaillée, distinguant cinq états différents : fortement malveillants, légèrement malveillants, fortement suspects, légèrement suspects et authentiques. L'état d'un véhicule à un instant t+1 dépendait de son état à un instant t. Les résultats de nos simulations ont démontré que notre modèle permettait d'atténuer de manière proactive les attaques DDoS avec un taux de fiabilité élevé.

Dans le chapitre 4, nous avons présenté notre modèle de confiance décentralisé, utilisant la technologie Blockchain et des contrats intelligents pour établir un système de gestion de confiance robuste pour les véhicules connectés. Nous avons développé quatre contrats intelligents à cet effet. Le premier contrat gérait les valeurs de notation des véhicules participants, tandis que le deuxième était chargé de gérer les pseudo-identités des véhicules au sein du réseau. Le troisième contrat contrôlait la gestion des accès des entités du réseau. Enfin, le dernier contrat intelligent gérait la participation des véhicules au réseau en ajoutant ou supprimant le pseudo-identifiant des véhicules dont la valeur de notation était respectivement supérieure ou inférieure à un seuil prédéfini. Ainsi, seuls les véhicules authentifiés et hautement fiables étaient autorisés à communiquer avec d'autres entités au sein de notre architecture automobile.

Dans le chapitre 5, nous avons introduit un système de sécurité et de préservation de la confidentialité novateur en combinant l'apprentissage fédéré avec la puissance de la Blockchain. Dans cette contribution, nous présentons un nouveau système de détection d'intrusion où la phase de formation ne repose pas uniquement sur une entité centrale, mais s'effectue au sein des véhicules connectés. Le processus d'apprentissage fédéré commence par la formation de modèles locaux dans les véhicules authentifiés. Ensuite, le SDNC (Software-Defined Network Controller) gère l'agrégation des modèles locaux formés pour sélectionner le meilleur modèle, qui est ensuite diffusé à tous les nœuds du réseau. L'intégration de la Blockchain et des contrats intelligents fournit une plateforme déterministe, sécurisée et mise à jour pour gérer les modèles en sécurisant les mises à jour des modèles échangées entre les véhicules connectés et le SDNC. Notre contribution améliore de manière significative le comportement autonome des véhicules connectés tout en renforçant la confidentialité des conducteurs.

Notre thèse a pour objectif d'améliorer la sécurité des véhicules connectés en développant des modèles visant à sécuriser les communications entre les composants réseau des réseaux de véhicules. Cependant, il reste encore des défis à relever. Cette section aborde certains défis majeurs et évoque des orientations de recherche futures pour renforcer la sécurité et la préservation de la confidentialité au sein des réseaux de véhicules. Nous discutons des solutions basées sur l'apprentissage fédéré, des approches de clustering, de la gestion de la consommation d'énergie, ainsi que de l'intégration des technologies émergentes et des solutions basées sur les enchères.

Dans le cadre de cette thèse, nous avons introduit un modèle léger de prédiction et de détection des attaques DDoS dans les réseaux véhiculaires et avons mené des simulations. Cependant, nous avons constaté que ses performances se réduisent lorsqu'il s'agit de garantir une évolutivité efficace. Notre perspective pour cette contribution consiste à développer un modèle qui améliore cette évolutivité. Les réseaux de véhicules sont des réseaux à grande échelle, souvent présents dans des zones urbaines denses, telles que les grandes villes, les autoroutes, les centres-villes, etc. En conséquence, une quantité considérable de données est traitée rapidement par chaque nœud. Le Machine Learning est l'un des outils techniques en croissance la plus rapide, ce qui le rend particulièrement adapté pour gérer ces énormes volumes de

données en un temps minimum. Ce paradigme permettra au système d'apprendre et d'améliorer automatiquement sa sécurité en se basant sur les données traitées précédemment. L'intégration du potentiel des techniques basées sur l'intelligence artificielle dans la gestion de la confiance des réseaux de véhicules améliore considérablement l'efficacité du réseau. Le Federated Learning (FL) représente une approche d'apprentissage automatique décentralisée qui résout les problèmes de formation centralisée des modèles. Dans ce cadre, tous les participants du réseau peuvent contribuer au développement du modèle global sans avoir à partager leurs données. Au sein des réseaux de véhicules, les nœuds participants peuvent occuper des rôles différents. Par conséquent, le FL conduit à des formulations et des modèles de confiance robustes qui dépendent de méthodes intelligentes distribuées, utilisant divers paramètres et métriques.

Dans le contexte de l'Internet des Véhicules (IoV), il est fréquent que les véhicules connectés authentifiés dans un domaine aient besoin d'être réauthentifiés dans un autre. Ce processus est défini comme le protocole inter-domaines, et il revêt une grande importance dans l'IoV, où les véhicules doivent souvent traverser différents domaines. Traditionnellement, le système d'infrastructure à clé publique (PKI) est couramment utilisé pour résoudre les problèmes liés à l'authentification de l'identité et à la confiance en matière de sécurité des véhicules connectés. Cependant, le système PKI présente des défis notables, notamment une autorité de certification (CA) excessivement centralisée, des interactions fréquentes entre domaines pour la gestion des certificats, des coûts de gestion élevés en raison du volume important d'authentifications, des chemins d'authentification complexes entre domaines, des risques de fuite de confidentialité, et une surcharge des réseaux. Dans le cadre de nos futurs travaux, nous nous efforçons de développer une solution basée sur la technologie blockchain pour résoudre ces problèmes. Notre approche inclut la création d'un système de gestion des identités PKI léger et une architecture d'authentification reposant sur des contrats intelligents. Cette solution vise à réduire la charge lourde imposée par les autorités de certification qui contrôlent directement le cycle de vie des certificats numériques.

Les réseaux de véhicules sont connus pour leur grande extensibilité. Cependant, une perspective générale sur le long terme est d'assurer l'efficacité énergétique de ces systèmes constitue un défi, en particulier en raison du volume considérable de données échangées entre les composants du réseau. Chaque nouveau mécanisme ou déploiement technologique dans les réseaux de véhicules semble entraîner une augmentation directe de la surcharge de communication et de la complexité temporelle, ce qui rend particulièrement difficile la satisfaction des exigences des applications en temps réel. Notre objectif est de trouver un équilibre optimal entre l'intégration de technologies émergentes et l'efficacité énergétique. Nous préconisons des approches légères pour réduire la consommation énergétique du système.
Notre premier objectif à court terme est de fusionner le paradigme du clustering avec la gestion décentralisée de la confiance, ce qui contribuera à améliorer la fiabilité du système, en particulier lors de l'intégration de technologies émergentes et décentralisées telles que le SDN ou la Blockchain. Ces technologies sont susceptibles d'améliorer les performances et la coordination entre les différents Cluster Heads (CH) et Cluster Members (CM) au sein des réseaux de véhicules. Dans cette perspective, nous cherchons à intégrer la métrique de confiance dans le processus de formation de clusters et la sélection des chefs de cluster. Ainsi, le nœud affichant la valeur de confiance la plus élevée sera élu chef de cluster. De plus, nous nous intéressons au développement d'un mécanisme de sauvegarde pour les Cluster Heads, afin de maintenir la stabilité des clusters au sein de l'IoV.

Enfin, nous examinons la répartition des mécanismes de ressources dans l'IoV (Internet des Véhicules) car nous avons remarqué que la distribution déséquilibrée des ressources et des incitations dans les réseaux de véhicules ouvre la voie à des attaques DDoS de grande ampleur. Dans une deuxième future perspective à court terme de ce travail, nous envisageons de fusionner le concept d'enchères avec la technologie blockchain dans les réseaux de véhicules. Dans ce scénario, une entité centrale serait chargée de fournir des ressources aux nœuds participants en fonction de leurs offres. Le fournisseur de services attribuerait les ressources au véhicule offrant la meilleure enchère à chaque tour d'enchères. Cependant, les véhicules malveillants chercheraient à falsifier les enchères des autres véhicules pour gagner à chaque fois, s'accaparant égoïstement toutes les unités de ressources. Notre objectif est de mettre en place un solide système de défense contre les cybermenaces, basé sur la théorie des jeux bayésienne, qui permet au système de détecter les nœuds malveillants. De plus, nous cherchons à développer un système de réputation, où les véhicules qui utilisent la majorité des unités demandées ou allouées seront considérés comme des nœuds honnêtes, et leur score de réputation sera augmenté.

# Bibliographie


[1] The World Health Organisation, Road traffic injuries, https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries

[2] H. Zhou, W. Xu, J. Chen and W. Wang, "Evolutionary V2X Technologies Toward the Internet of Vehicles : Challenges and Opportunities," in Proceedings of the IEEE, vol. 108, no. 2, pp. 308-323, Feb. 2020, doi : 10.1109/JPROC.2019.2961937.

[3] Tesla cars https://www.caranddriver.com/tesla

[4] Cyber Attacks in Connected Cars - What Tesla Did Differently to Win, 2017. https://www.appknox.com/blog/cyber-attacks-in-connected-cars

[5] New attack can unlock and start a Tesla Model Y in seconds,2022.https://www.theverge.com/2022/9/12/23348765/tesla-model-y-unlock-drive-car-thief-nfc-relay-attack

[6] M. Ren, J. Zhang, L. Khoukhi, H. Labiod and V. Vèque, A Unified Framework in Vehicular Ad Hoc Networks, in IEEE Transactions on Intelligent Transportation Systems, vol.19, no.5, pp.1401-1414, May 2018.

[7] Ren, M., Zhang, J., Khoukhi, L. et al. A review of clustering algorithms in Vehicular networks. Ann. Telecommun, 2021. https ://doi.org/10.1007/s12243-020-00831-x

[8] M. A. Togou, L. Khoukhi and A. Hafid, "IEEE 802.11p EDCA performance analysis for vehicle-to-vehicle infotainment applications," 2017 IEEE International Conference on Communications (ICC), 2017, pp. 1-6, doi : 10.1109/ICC.2017.7996759.

[9] M. Ren, L. Khoukhi, H. Labiod, J. Zhang and V. Veque, "A new mobility-based clustering algorithm for vehicular ad hoc networks (Vehicular Networks)," NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, 2016, pp. 1203-1208, doi : 10.1109/NOMS.2016.7502988.

[10] Mengying Ren, Lyes Khoukhi, Houda Labiod, Jun Zhang, Véronique Vèque,"A mobility-based scheme for dynamic clustering in vehicular ad-hoc networks (Vehicular Networks)",Vehicular Communications,Volume 9,Pages 233-241, 2017. https ://doi.org/10.1016/j.vehcom.2016.12.003.

[11] A. Tahmasbi-Sarvestani, Y. P. Fallah and V. Kulathumani, "Network-Aware Double-Layer Distance-Dependent Broadcast Protocol for Vehicular networks," in IEEE Transactions on Vehicular Technology, vol. 64, no. 12, pp. 5536-5546, Dec. 2015, doi : 10.1109/TVT.2015.2487998.

[12] S. U. Bhover, A. Tugashetti and P. Rashinkar, "V2X communication protocol in Vehicular Network for co-operative intelligent transportation system," 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2017, pp. 602-607, doi : 10.1109/ICIMIA.2017.7975531.

[13] A. Ydenberg, N. Heir and B. Gill, "Security, SDN, and Vehicular Network technology of driver-less cars," 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 2018, pp. 313-316, doi : 10.1109/CCWC.2018.8301777.

[14] H. A. Khattak, S. U. Islam, I. U. Din and M. Guizani, "Integrating Fog Computing with Vehicular networks : A Consumer Perspective," in IEEE Communications Standards Magazine, vol. 3, no. 1, pp. 19-25, March 2019, doi : 10.1109/MCOMSTD.2019.1800050.

[15] M. Ren, J. Zhang, L. Khoukhi, H. Labiod and V. Veque, A Unified Framework in Vehicular Ad Hoc Networks, in IEEE Transactions on Intelligent Transportation Systems, vol.19, no.5, pp.1401-1414, May 2018.

[16] P. Tiwari and R. S. Kushwah, "Traffic analysis for Vehicular Network using WAVE and WiMAX," 2015 International Conference on Communication Networks (ICCN), 2015, pp. 343-346, doi : 10.1109/ICCN.2015.65.

[17] M. A. Togou, L. Khoukhi and A. Hafid, "IEEE 802.11p EDCA performance analysis for vehicle-to-vehicle infotainment applications," 2017 IEEE International Conference on Communications (ICC), 2017, pp.1-6,doi : 10.1109/ICC.2017.7996759.

[18] S. U. Bhover, A. Tugashetti and P. Rashinkar, "V2X communication protocol in Vehicular Network for co-operative intelligent transportation system," 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2017, pp. 602-607, doi : 10.1109/ICIMIA.2017.7975531.

[19] A. K. Goyal, A. Kumar Tripathi and G. Agarwal, "Security Attacks, Requirements and Authentication Schemes in Vehicular Network," 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2019, pp. 1-5, doi : 10.1109/ICICT46931.2019.8977656.

[20] B. Ayyappan and P. M. Kumar, "Vehicular Ad Hoc Networks (Vehicular Network) : Architectures, methodologies and design issues," 2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM), 2016, pp. 177-180, doi : 10.1109/ICONSTEM.2016.7560946.

[21] H. Amari, W. Louati, L. Khoukhi and L. H. Belguith, "Securing Software-Defined Vehicular Network Architecture against DDoS attack," 2021 IEEE 46th Conference on Local Computer Networks (LCN), 2021, pp. 653-656, doi : 10.1109/LCN52139.2021.9524953.

[22] P. Tyagi and D. Dembla, "Investigating the security threats in Vehicular ad hoc Networks (Vehicular Networks) : Towards security engineering for safer on-road transportation," 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2014, pp. 2084-2090, doi : 10.1109/ICACCI.2014.6968313.

[23] World Health Organization. Death on the Roads. Based on the WHO Global Status Report on Road Safety 2018 ; World Health Organization : Geneva, Switzerland, 2018. Available online : https://extranet.who.int/roadsafety/death-on-the-roads/deaths

[24] S. Zarbi, S. A. Mortazavi and P. Salehpour, "Security Analysis of an Efficient Authentication Scheme for Vehicular Ad Hoc Networks," 2020 17th International ISC Conference on Information Security and Cryptology (ISCISC), 2020, pp. 44-47, doi : 10.1109/ISCISC51277.2020.9261912.

[25] M. Asghar, R. R. M. Doss and L. Pan, "A Scalable and Efficient PKI Based Authentication Protocol for Vehicular networks," 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), 2018, pp. 1-3, doi : 10.1109/ATNAC.2018.8615224.

[26] J. Zhang and Q. Zhang, "On the Security of a Lightweight Conditional Privacy-Preserving Authentication in Vehicular networks," in IEEE Transactions on Information Forensics and Security, doi : 10.1109/TIFS.2021.3066277.

[27] B. Pooja, M. M. M. Pai, R. M. Pai, N. Ajam and J. Mouzna, "Mitigation of insider and outsider DoS attack against signature based authentication in Vehicular networks," 2014 Asia-Pacific Conference on Computer Aided System Engineering (APCASE), 2014, pp. 152-157, doi : 10.1109/APCASE.2014.6924490.

[28] B. K. Chaurasia, S. Verma and G. S. Tomar, "Trust Computation in Vehicular networks," 2013 International Conference on Communication Systems and Network Technologies, 2013, pp. 468-471, doi : 10.1109/CSNT.2013.103.

[29] H. Sateesh and P. Zavarsky, "State-of-the-Art Vehicular Network Trust Models : Challenges and Recommendations," 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2020, pp. 0757-0764, doi : 10.1109/IEMCON51383.2020.9284953.

[30] H. Amari, L. Khoukhi and L. H. Belguith, "Prediction and detection model for hierarchical Software-Defined Vehicular Network," 2022 IEEE 47th Conference on Local Computer Networks (LCN), 2022, pp. 463-470, doi : 10.1109/LCN53696.2022.9843483.

[31] Deeksha, A. Kumar and M. Bansal, "A review on Vehicular Network security attacks and their countermeasure," 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), 2017, pp. 580-585, doi : 10.1109/ISPCC.2017.8269745.

[32] T. Pavithra and B. S. Nagabhushana, "A Survey on Security in Vehicular networks," 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), 2020, pp. 881-889, doi : 10.1109/ICIRCA48905.2020.9182823.

[33] N. Phull and P. Singh, "A Review on Security Issues in Vehicular networks," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 1084-1088.

[34] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil and I. H. Hasbullah, "Security and Privacy Schemes in Vehicular Ad-Hoc Network With Identity-Based Cryptography Approach : A Survey," in IEEE Access, vol. 9, pp. 121522-121531, 2021, doi : 10.1109/ACCESS.2021.3109264.

[35] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar and A. Basir, "A Survey on Privacy-Preserving Authentication Schemes in Vehicular networks : Attacks, Challenges and Open Issues," in IEEE Access, vol. 9, pp. 153701-153726, 2021, doi : 10.1109/ACCESS.2021.3125521.

[36] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah and S. Manickam, "Survey of Authentication and Privacy Schemes in Vehicular ad hoc Networks," in IEEE Sensors Journal, vol. 21, no. 2, pp. 2422-2433, 15 Jan.15, 2021, doi : 10.1109/JSEN.2020.3021731.

[37] R. Hussain, J. Lee and S. Zeadally, "Trust in Vehicular Network : A Survey of Current Solutions and Future Research Opportunities," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 5, pp. 2553-2571, May 2021, doi : 10.1109/TITS.2020.2973715.

[38] Z. Lu, G. Qu and Z. Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy," in IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 2, pp. 760-776, Feb. 2019, doi : 10.1109/TITS.2018.2818888.

[39] A. Ahamed and H. Vakilzadian, "Issues and Challenges in Vehicular Network Routing Protocols," 2018 IEEE International Conference on Electro/Information Technology (EIT), 2018, pp. 0723-0728, doi : 10.1109/EIT.2018.8500180.

[40] A. Boualouache, S. -M. Senouci and S. Moussaoui, "A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks," in IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 770-790, Firstquarter 2018, doi : 10.1109/COMST.2017.2771522.

[41] G. M. Jinarajadasa and S. R. Liyange, "A survey on applying machine learning to enhance trust in mobile adhoc networks," 2020 International Research Conference on Smart Computing and Systems Engineering (SCSE), 2020, pp. 195-201, doi : 10.1109/SCSE49731.2020.9313021.

[42] M. Gillani, A. Ullah and H. A. Niaz, "Trust Management Schemes for Secure Routing in Vehicular networks — A Survey," 2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), 2018, pp. 1-6, doi : 10.1109/MACS.2018.8628440.

[43] SHAFIQ, Zeeshan, ZAFAR, Mohammad Haseeb, et QAZI, Abdul Baseer. QoS in Vehicular Ad Hoc Networks–A Survey. Journal of Information Communication Technologies and Robotic Applications, 2018, p. 48-58.

[44] Z. Wang, Y. Wang, Y. Zhang, Y. Liu, C. Ma, H. Wang, A brief survey on cyber security attack entrances and protection strategies of intelligent connected vehicle, in : International Conference on Smart Computing and Communication, 2019, pp. 73–82.

[45] SOUISSI, Ilhem, AZZOUNA, Nadia Ben, et BERRADIA, Tahar. Trust management in vehicular ad hoc networks : a survey. International Journal of Ad Hoc and Ubiquitous Computing, 2019, vol. 31, no 4, p. 230-243.

[46] Akash Vaibhav, Dilendra Shukla, Sanjoy Das, Subrata Sahana, Prashant Johri,"Security Challenges, Authentication, Application and Trust Models for Vehicular Ad Hoc Network- A Survey", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.7, No.3, pp.36-48, 2017.DOI : 10.5815/ijwmt.2017.03.04

[47] N. H. Hussein, C. T. Yaw, S. P. Koh, S. K. Tiong and K. H. Chong, "A Comprehensive Survey on Vehicular Networking : Communications, Applications, Challenges, and Upcoming Research Directions," in IEEE Access, vol. 10, pp. 86127-86180, 2022, doi : 10.1109/ACCESS.2022.3198656.

[48] Arif, M., Wang, G., Bhuiyan, M. Z. A., Wang, T., & Chen, J. (2019). A survey on security attacks in Vehicular networks : Communication, applications and challenges. Vehicular Communications, 19, 100179.

[49] Y. Fan, X. Xiao and W. Feng, "An Anti-Jamming Game in Vehicular Network Platoon with Reinforcement Learning," 2018 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2018, pp. 1-2, doi : 10.1109/ICCE-China.2018.8448435.

[50] S. S. Chhatwal and M. Sharma, "Detection of impersonation attack in Vehicular networks using BUCK Filter and Vehicular Network Content Fragile Watermarking (VCFW)," 2015 International Conference on Computer Communication and Informatics (ICCCI), 2015, pp. 1-5, doi : 10.1109/ICCCI.2015.7218093.

[51] X. Lin and X. Li, “Authentication in vehicular ad hoc networks,” IEEE Transactions on Vehicular Technology, vol. 62, no. 7, pp. 3339–3348, (2013).

[52] MEJRI, Mohamed Nidhal, BEN-OTHMAN, Jalel, et HAMDI, Mohamed. Survey on Vehicular Network security challenges and possible cryptographic solutions. Vehicular Communications, 2014, vol. 1, no 2, p. 53-66.

[53] D. P. Choudhari and S. S. Dorle, "Maximization of packet delivery ratio for DADCQ protocol after removal of Eavesdropping and DDoS attacks in Vehicular Network," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-8, doi : 10.1109/ICCCNT45670.2019.8944485.

[54] 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.

[55] Hafiz M. A pattern language for developing privacy enhancing technologies. Softw Pract Exp. ,43(7) :769-787, (2013).

[56] N. -W. Lo and H. -C. Tsai, "Illusion Attack on Vehicular Network Applications - A Message Plausibility Problem," 2007 IEEE Globecom Workshops, 2007, pp. 1-8, doi : 10.1109/GLOCOMW.2007.4437823.

[57] A M. N. Mejri and J. Ben-Othman, "GDVAN : A New Greedy Behavior Attack Detection Algorithm for Vehicular networks," in IEEE Transactions on Mobile Computing, vol. 16, no. 3, pp. 759-771, (2017).

[58] G. -M. Hoang, B. Denis, J. Härri and D. T. M. Slock, "Robust data fusion for cooperative vehicular localization in tunnels," 2017 IEEE Intelligent Vehicles Symposium (IV), 2017, pp. 1372-1377, doi : 10.1109/IVS.2017.7995902.

[59] Su, Z., Hui, Y., Luan, T.H., Liu, Q., Xing, R. (2021). Reputation Based Content Delivery in Information Centric Vehicular networks. In : The Next Generation Vehicular networks, Modeling, Algorithm and Applications. Wireless Networks. Springer, Cham. https://doi.org/10.1007/978-3-030-56827-6-2

[60] L. Wei, J. Cui, Y. Xu, J. Cheng and H. Zhong, "Secure and Lightweight Conditional Privacy-Preserving Authentication for Securing Traffic Emergency Messages in Vehicular networks," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1681-1695, 2021, doi : 10.1109/TIFS.2020.3040876.

[61] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan and A. Aldegheishem, "Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and connected vehicles," in IEEE Access, vol. 8, pp. 199618-199628, 2020, doi : 10.1109/ACCESS.2020.3034327.

[62] Laxmi V, Lal C, Gaur MS, Mehta D. JellyFish attack : analysis, detection and countermeasure in TCP-based MANET. J Inform Secur Appl. ; 22 :99-112, (2015).

[63] N. Schweitzer, A. Stulman, R. D. Margalit and A. Shabtai, "Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks," in IEEE Transactions on Mobile Computing, vol. 16, no. 8, pp. 2174-2183, 1 Aug. 2017, doi : 10.1109/TMC.2016.2622707.

[64] K. Stepień and A. Poniszewska-Marańda, "Analysis of security methods in Vehicular Ad-Hoc Network against Worm Hole and Gray Hole attacks," 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), 2020, pp. 371-378, doi : 10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00072.

[65] P. K. Singh, A. Agarwal, G. Nakum, D. B. Rawat and S. Nandi, "MPFSLP : Masqueraded Probabilistic Flooding for Source-Location Privacy in Vehicular networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 10, pp. 11383-11393, Oct. 2020, doi : 10.1109/TVT.2020.3009763.

[66] M. A. Al-shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah and M. M. Hamdi, "Review of Prevention schemes for Replay Attack in Vehicular Ad hoc Networks (Vehicular Networks)," 2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP), 2020, pp. 394-398, doi : 10.1109/ICICSP50920.2020.9232047.

[67] S. Bittl, A. A. Gonzalez, M. Myrtus, H. Beckmann, S. Sailer and B. Eissfeller, "Emerging attacks on Vehicular Network security based on GPS Time Spoofing," 2015 IEEE Conference on Communications and Network Security (CNS), 2015, pp. 344-352, doi : 10.1109/CNS.2015.7346845.

[68] A. Singh and P. Sharma, "A novel mechanism for detecting DOS attack in Vehicular Network using Enhanced Attacked Packet Detection Algorithm (EAPDA)," 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS), 2015, pp. 1-5, doi : 10.1109/RAECS.2015.7453358.

[69] M. Poongodi, M. Hamdi, A. Sharma, M. Ma and P. K. Singh, "DDoS Detection Mechanism Using Trust-Based Evaluation System in Vehicular Network," in IEEE Access, vol. 7, pp. 183532-183544, 2019, doi : 10.1109/ACCESS.2019.2960367.

[70] Ahmed W, Elhadef M. Securing Intelligent Vehicular Ad Hoc Networks : A Survey. In : Park J, Loia V, Yi G, Sung Y. (eds) Advances in Computer Science and Ubiquitous Computing. CUTE 2017, CSA. Lecture Notes in Electrical Engineering, Springer, Singapore, 474 :6–14, (2017).

[71] M. Azees, L. Jegatha Deborah, and P. Vijayakumar, "Comprehensive survey on security services in vehicular adhoc networks," IET Intelligent Transport Systems, vol. 10, no. 6, pp. 379–388, (2016).

[72] H. Xia, S. -s. Zhang, Y. Li, Z. -k. Pan, X. Peng and X. -z. Cheng, "An Attack-Resistant Trust Inference Model for Securing Routing in Vehicular Ad Hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 68, no. 7, pp. 7108-7120, July 2019, doi : 10.1109/TVT.2019.2919681.

[73] Al Falasi, H., Mohamed, N. (2015). Similarity-Based Trust Management System for Detecting Fake Safety Messages in Vehicular networks. In : Hsu, CH., Xia, F., Liu, X., Wang, S. (eds) Internet of Vehicles - Safe and Intelligent Mobility. IOV 2015. Lecture Notes in Computer Science(), vol 9502. Springer, Cham. https://doi.org/10.1007/978-3-319-27293-1-24

[74] J. Cui, X. Zhang, H. Zhong, Z. Ying and L. Liu, "RSMA : Reputation System-Based Lightweight Message Authentication Framework and Protocol for 5G-Enabled Vehicular networks," in IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6417-6428, Aug. 2019, doi : 10.1109/JIOT.2019.2895136.

[75] H. Hu, R. Lu, Z. Zhang and J. Shao, "REPLACE : A Reliable Trust-Based Platoon Service Recommendation Scheme in Vehicular Network," in IEEE Transactions on Vehicular Technology, vol. 66, no. 2, pp. 1786-1797, Feb. 2017, doi : 10.1109/TVT.2016.2565001.

[76] K. Zaidi, M. Milojevic, V. Rakocevic and M. Rajarajan, "Data-centric Rogue Node Detection in Vehicular networks," 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, 2014, pp. 398-405, doi : 10.1109/TrustCom.2014.51.

[77] Shaikh, R. A., and Alzahrani, A. S. (2014), Intrusion-aware trust model for vehicular ad hoc networks, Security Comm. Networks, 7, pages 1652– 1669, doi : 10.1002/sec.862

[78] Shaikh, R.A., Alzahrani, A.S. (2013). Trust Management Method for Vehicular Ad Hoc Networks. In : Singh, K., Awasthi, A.K. (eds) Quality, Reliability, Security and Robustness in Heterogeneous Networks. QShine 2013. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 115. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37949-9-70

[79] Y. -C. Wei and Y. -M. Chen, "An Efficient Trust Management System for Balancing the Safety and Location Privacy in Vehicular networks," 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 393-400, doi : 10.1109/TrustCom.2012.79.

[80] Y. -C. Wei and Y. -M. Chen, "Adaptive decision making for improving trust establishment in Vehicular Network," The 16th Asia-Pacific Network Operations and Management Symposium, 2014, pp. 1-4, doi : 10.1109/APNOMS.2014.6996523.

[81] Wenyuan Li, Ke Gong, Qingjiao Li, Frank Alber, Xianghong Jasmine Zhou, Hi-Corrector : a fast, scalable and memory-efficient package for normalizing large-scale Hi-C data, Bioinformatics, Volume 31, Issue 6, 15 March 2015, Pages 960–962, https://doi.org/10.1093/bioinformatics/btu747

[82] Płaczek, B., Bernas, M. (2016). Detection of Malicious Data in Vehicular Ad Hoc Networks for Traffic Signal Control Applications. In : Gaj, P., Kwiecień, A., Stera, P. (eds) Computer Networks. CN 2016. Communications in Computer and Information Science, vol 608. Springer, Cham. https://doi.org/10.1007/978-3-319-39207-3-7

[83] Chen Y.M., Wei Y.C., Abeacon-based trust management system for enhancing user centric location privacy in Vehicular networks, J. Commun. Netw., 15 (2) (2013), pp. 153-163

[84] J. Pawlick, J. Chen and Q. Zhu, "iSTRICT : An Interdependent Strategic Trust Mechanism for the Cloud-Enabled Internet of Controlled Things," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 6, pp. 1654-1669, June 2019, doi : 10.1109/TIFS.2018.2883272.

[85] Chaurasia, B.K., Sharma, K. (2019). Trust Computation in Vehicular Network Cloud. In : Gavrilova, M., Tan, C. (eds) Transactions on Computational Science XXXIV. Lecture Notes in Computer Science(), vol 11820. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-59958-7-5

[86] X. Chen and L. Wang, "A Cloud-Based Trust Management Framework for Vehicular Social Networks," in IEEE Access, vol. 5, pp. 2967-2980, 2017, doi : 10.1109/ACCESS.2017.2670024.

[87] S. S. Mudengudi and M. S. Kakkasageri, "Establishing trust between vehicles in vehicular clouds : An agent based approach," 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), 2017, pp. 529-533, doi : 10.1109/SmartTechCon.2017.8358428.

[88] D. Zhang, F. R. Yu and R. Yang, "A Machine Learning Approach for Software-Defined Vehicular Ad Hoc Networks with Trust Management," 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1-6, doi : 10.1109/GLOCOM.2018.8647426.

[89] D. Zhang, F. R. Yu, R. Yang and L. Zhu, "Software-Defined Vehicular networks With Trust Management : A Deep Reinforcement Learning Approach," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 2, pp. 1400-1414, Feb. 2022, doi : 10.1109/TITS.2020.3025684.

[90] D. Zhang, F.R. Yu, Z. Wei, A. Boukerche, Software-defined vehicular ad hoc networks with trust management, in : Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular networks and Applications, 2016, pp. 41–49.

[91] L. Alouache, M. Maachaoui, R. Chelouah, Securing hybrid SDN-based geographic routing protocol using a distributed trust model, Adv. Sci. Technol. Eng. Syst. J. (2020).

[92] X. Huang, R. Yu, J. Kang, Y. Zhang, Distributed reputation management for secure and efficient vehicular edge computing and networks, IEEE Access 5 (2017) 25408–25420.

[93] F. Dewanta and M. Mambo, "Bidding Price-Based Transaction : Trust Establishment for Vehicular Fog Computing Service in Rural Area," 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2019, pp. 882-887, doi : 10.1109/PERCOMW.2019.8730830.

[94] S. A. Soleymani et al., “A Trust Model Using Edge Nodes and a Cuckoo Filter for Securing Vehicular Network under the NLoS Condition,” Symmetry, vol. 12, no. 4, p. 609, Apr. 2020, doi : 10.3390/sym12040609.

[95] R. J. Atwa, P. Flocchini and A. Nayak, "A Fog-based Reputation Evaluation Model for Vehicular networks," 2021 International Symposium on Networks, Computers and Communications (ISNCC), 2021, pp. 1-7, doi : 10.1109/ISNCC52172.2021.9615820.

[96] Z. Lu, Q. Wang, G. Qu and Z. Liu, "BARS : A Blockchain-Based Anonymous Reputation System for Trust Management in Vehicular networks," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 98-103, doi :10.1109/TrustCom/BigDataSE.2018.00025.

[97] Y. Zou, F. Shen, F. Yan, J. Lin and Y. Qiu, "Reputation-Based Regional Federated Learning for Knowledge Trading in Blockchain-Enhanced IoV," 2021 IEEE Wireless Communications and Networking Conference (WCNC), 2021, pp. 1-6, doi : 10.1109/WCNC49053.2021.9417347.

[98] C. Zhang, W. Li, Y. Luo and Y. Hu, "AIT : An AI-Enabled Trust Management System for Vehicular networks Using Blockchain Technology," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3157-3169, 1 March1, 2021, doi : 10.1109/JIOT.2020.3044296.

[99] Z. Yang, K. Yang, L. Lei, K. Zheng and V. C. M. Leung, "Blockchain-Based Decentralized Trust Management in Vehicular networks," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1495-1505, April 2019, doi : 10.1109/JIOT.2018.2836144.

[100] S. Oubabas, R. Aoudjit, J.J. Rodrigues, S. Talbi, Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme, Veh. Commun. 13 (2018) 128–138.

[101] A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng and S. A. Siddiqui, "A Hybrid Trust Management Heuristic for Vehicular networks," 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2019, pp. 748-752, doi : 10.1109/PERCOMW.2019.8730675.

[102] F. A. Ghaleb et al., “Misbehavior-Aware On-Demand Collaborative Intrusion Detection System Using Distributed Ensemble Learning for Vehicular Network,” Electronics, vol. 9, no. 9, p. 1411, Sep. 2020, doi : 10.3390/electronics9091411.

[103] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta and C. -H. Hsu, "Efficient and Secure Routing Protocol Based on Artificial Intelligence Algorithms With UAV-Assisted for Vehicular Ad Hoc Networks in Intelligent Transportation Systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4757-4769, July 2021, doi : 10.1109/TITS.2020.3041746.

[104] S. A. Soleymani et al., "A Secure Trust Model Based on Fuzzy Logic in Vehicular Ad Hoc Networks With Fog Computing," in IEEE Access, vol. 5, pp. 15619-15629, 2017, doi : 10.1109/ACCESS.2017.2733225.

[105] M. M. Hasan, M. Jahan, S. Kabir and C. Wagner, "A Fuzzy Logic-Based Trust Estimation in Edge-Enabled Vehicular Ad Hoc Networks," 2021 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2021, pp. 1-8, doi : 10.1109/FUZZ45933.2021.9494428.

[106] G. M and C. Gomathy, "Fuzzy based Trusted Communication in Vehicular Ad hoc Network," 2022 2nd International Conference on Intelligent Technologies (CONIT), 2022, pp. 1-4, doi : 10.1109/CONIT55038.2022.9847823.

[107] Y. Inedjaren, B. Zeddini, M. Maachaoui and J. -P. Barbot, "Securing Intelligent Communications on the Vehicular AdHoc Networks using Fuzzy Logic Based Trust OLSR," 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), 2019, pp. 1-6, doi : 10.1109/AICCSA47632.2019.9035241.

[108] T. Halabi and M. Zulkernine, "Trust-Based Cooperative Game Model for Secure Collaboration in the Internet of Vehicles," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 2019, pp. 1-6, doi : 10.1109/ICC.2019.8762069.

[109] B. Subba, S. Biswas, S. Karmakar, A game theory based multi layered intrusion detection framework for Vehicular Network, Future Gener. Comput. Syst. 82 (2018) 12–28.

[110] Z. Tian, X. Gao, S. Su, J. Qiu, X. Du and M. Guizani, "Evaluating Reputation Management Schemes of Internet of Vehicles Based on Evolutionary Game Theory," in IEEE Transactions on Vehicular Technology, vol. 68, no. 6, pp. 5971-5980, June 2019, doi : 10.1109/TVT.2019.2910217.

[111] N. Fan, C.Q. Wu, On trust models for communication security in vehicular ad-hoc networks, Ad Hoc Netw. 90 (2019) 101740.

[112] Haddaji, A., Ayed, S., Chaari, L. (2022). Federated Learning with Blockchain Approach for Trust Management in IoV. In : Barolli, L., Hussain, F., Enokido, T. (eds) Advanced Information Networking and Applications. AINA 2022. Lecture Notes in Networks and Systems, vol 449. Springer, Cham. https://doi.org/10.1007/978-3-030-99584-3-36

[113] G. Khayat, C. X. Mavromoustakis, G. Mastorakis, J. M. Batalla, H. Maalouf and E. Pallis, "Vehicular Network Clustering Based on Weighted Trusted Cluster Head Selection," 2020 International Wireless Communications and Mobile Computing (IWCMC), 2020, pp. 623-628, doi : 10.1109/IWCMC48107.2020.9148339.

[114] H. N. Abdulrazzak, N. M. L. Tan and N. A. Mohd. Radzi, "Minimizing Energy Consumption in Roadside Unit of Zigzag Distribution Based on RS-LS Technique," 2021 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS), 2021, pp. 169-173, doi : 10.1109/I2CACIS52118.2021.9495853.

[115] P. Gu, R. Khatoun, Y. Begriche, and A. Serhrouchni, “Vehicle driving pattern based sybil attack detection,” in High Performance Computing and Communications ; IEEE 14th International Conference on Smart City ; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016

[116] Z. A. El Houda, A. S. Hafid and L. Khoukhi, "A Novel Machine Learning Framework for Advanced Attack Detection using SDN," 2021 IEEE Global Communications Conference (GLOBECOM), 2021, pp. 1-6, doi : 10.1109/GLOBECOM46510.2021.9685643.

[117] R. Khatoun, P. Gut, R. Doulami, L. Khoukhi and A. Serhrouchni, "A reputation system for detection of black hole attack in vehicular networking," 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015, pp. 1-5, doi : 10.1109/SSIC.2015.7245328.IEEE 18th International Conference on IEEE, 2016, pp. 1282–1288.

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

[119] M. Mansouri, L. Khoukhi, H. Nounou and M. Nounou, "Secure and robust clustering for quantized target tracking in wireless sensor networks," in Journal of Communications and Networks, vol. 15, no. 2, pp. 164-172, April 2013, doi : 10.1109/JCN.2013.000029.

[120] K. Assafra, B. Alaya and M. Abid, "Privacy preservation and security management in Vehicular Network based to Software Defined Network," 2022 IEEE Wireless Communications and Networking Conference (WCNC), 2022, pp. 96-101, doi : 10.1109/WCNC51071.2022.9771705.

[121] H. Amari, W. Louati, L. Khoukhi and L. H. Belguith, "Securing Software-Defined Vehicular Network Architecture against DDoS attack," 2021 IEEE 46th Conference on Local Computer Networks (LCN), 2021, pp. 653-656, doi : 10.1109/LCN52139.2021.9524953.

[122] Islam, M. M., Khan, M. T. R., Saad, M. M., & Kim, D. (2021). Software-defined vehicular network (SDVN) : A survey on architecture and routing. Journal of Systems Architecture, 114, 101961.

[123] "Cisco annual internet report (2018–2023) white paper,https://www.cisco.com/c/en/us/solutions/collateral/execuiveperspectives/annual-internet-report/white-paper-c11-741490.hml.

[124] Q. Yan, F. R. Yu, Q. Gong and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments : A Survey, Some Research Issues, and Challenges," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 602-622, Firstquarter 2016, doi : 10.1109/COMST.2015.2487361.

[125] A. Bhatia, K. Haribabu, K. Gupta and A. Sahu, "Realization of flexible and scalable Vehicular networks through SDN and virtualization," 2018 International Conference on Information Networking (ICOIN), 2018, pp. 280-282, doi : 10.1109/ICOIN.2018.8343125.

[126] K. Verma and H. Hasbullah, "Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in Vehicular Network," Security and Communication Networks, vol. 8, no. 5, pp. 864–878, 2015.

[127] S. A. Ghorsad, P. P. Karde, V. M. Thakare, and R. V. Dharaskar, "DoS attack detection in vehicular ad-hoc network using malicious node detection algorithm," International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE), vol. 3, p. 36, 2014.

[128] Ö. Cepheli, S. Büyükçorak, and G. Karabulut Kurt, "Hybrid Intrusion Detection System for DDoS Attacks," Journal of Electrical and Computer Engineering, vol. 2016, Article ID 1075648, 8 pages, 2016.

[129] A. Sinha and S. K. Mishra, "Queue Limiting Algorithm (QLA) for Protecting Vehicular Network from Denial of Service (DoS) Attack," International Journal of Computer Applications, vol. 86, no. 8, pp. 14–17, 2014.

[130] Z. He, J. Cao and X. Liu, "SDVN : enabling rapid network innovation for heterogeneous vehicular communication," in IEEE Network, vol. 30, no. 4, pp. 10-15, July-August 2016, doi : 10.1109/MNET.2016.7513858.

[131] Al-Heety, O. S., Zakaria, Z., Ismail, M., Shakir, M. M., Alani, S., & Alsariera, H. (2020). A Comprehensive Survey : Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET. IEEE Access, 8, 91028–91047. https ://doi.org/10.1109/ACCESS.2020.2992580

[132] Aloqaily, M., Elayan, H., & Guizani, M. (2023). C-HealthIER : A Cooperative Health Intelligent Emergency Response System for C-ITS. IEEE Transactions on Intelligent Transportation Systems, 24(2), 2111–2121. https ://doi.org/10.1109/TITS.2022.3141018

[133] Amari, H., Houda, Z. A. E., Khoukhi, L., & Belguith, L. H. (2023). Trust Management in Vehicular Ad-Hoc Networks : Extensive Survey. IEEE Access, 11, 47659–47680. https ://doi.org/10.1109/ACCESS.2023.3268991

[134] Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts. In Principles of Security and Trust. Heidelberg, 2, 164–186.

[135] Babbar, H., Bouachir, O., Rani, S., & Aloqaily, M. (2022). Evaluation of Deep Learning Models in ITS Software-Defined Intrusion Detection Systems. NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, 1–6. https ://doi.org/10.1109/NOMS54207.2022.9789829

[136] Common Weakness Enumeration (CWE). (n.d.). https ://cwe.mitre.org/

[137] El Houda, Z. A., Brik, B., & Khoukhi, L. (2022). Ensemble Learning for Intrusion Detection in SDN-Based Zero Touch Smart Grid Systems. 2022 IEEE 47th Conference on Local Computer Networks (LCN), 149–156. https ://doi.org/10.1109/LCN53696.2022.9843645

[138] El Houda, Z. A., Brik, B., Ksentini, A., & Khoukhi, L. (2023). A MEC-Based Architecture to Secure IoT Applications using Federated Deep Learning. IEEE Internet of Things Magazine, 6(1), 60–63. https ://doi.org/10.1109/IOTM.001.2100238

[139] El Houda, Z. A., Brik, B., & Senouci, S.-M. (2022). A Novel IoT-Based Explainable Deep Learning Framework for Intrusion Detection Systems. IEEE Internet of Things Magazine, 5(2), 20–23. https ://doi.org/10.1109/IOTM.005.2200028

[140] Elayan, H., Aloqaily, M., Salameh, H. B., & Guizani, M. (2021). Intelligent Cooperative Health Emergency Response System in Autonomous Vehicles. 2021 IEEE 46th Conference on Local Computer Networks (LCN), 293–298. https ://doi.org/10.1109/LCN52139.2021.9524950

[141] Ethereum. (n.d.). https://ethereum.org/en/

[142] Feng, C., Yu, K., Aloqaily, M., Alazab, M., Lv, Z., & Mumtaz, S. (2020). Attribute-Based Encryption With Parallel Outsourced Decryption for Edge Intelligent IoV. IEEE Transactions on Vehicular Technology, 69(11), 13784–13795. https ://doi.org/10.1109/TVT.2020.3027568

[143] Ganache. (n.d.). https://trufflframework.com/docs/ganache/overview

[144] Houda, Z. A. E., Beaugeard, J., Sauvêtre, Q., & Khoukhi, L. (2023). Towards a Secure and Scalable Access Control System Using Blockchain. 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 1–8. https ://doi.org/10.1109/ICBC56567.2023.10174880

[145] Houda, Z. A. E., Brik, B., & Khoukhi, L. (2022). "Why Should I Trust Your IDS ?" : An Explainable Deep Learning Framework for Intrusion Detection Systems in Internet of Things Networks. IEEE Open Journal of the Communications Society, 3, 1164–1176. https ://doi.org/10.1109/OJCOMS.2022.3188750

[146] Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., & Weil, T. (2011). Vehicular Networking : A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. IEEE Communications Surveys & Tutorials, 13(4), 584–616. https://doi.org/10.1109/SURV.2011.061411.00019

[147] Kazmi, S. M. A., Otoum, S., Hussain, R., & Mouftah, H. T. (2021). A Novel Deep Reinforcement Learning-based Approach for Task-offloading in Vehicular networks. 2021 IEEE Global Communications Conference (GLOBECOM), 1–6. https://doi.org/10.1109/GLOBECOM46510.2021.9685073

[148] Kerrache, C. A., Calafate, C. T., Cano, J.-C., Lagraa, N., & Manzoni, P. (2016). Trust Management for Vehicular networks : An Adversary-Oriented Overview. IEEE Access, 4, 9293–9307. https://doi.org/10.1109/ACCESS.2016.2645452

[149] Khattak, H. A., Raja, F. Z., Aloqaily, M., & Bouachir, O. (2021). Efficient In-Network Caching in NDN-based connected vehicles. 2021 IEEE Global Communications Conference (GLOBECOM), 01–06. https ://doi.org/10.1109/GLOBECOM46510.2021.9685200

[150] Kolosz, B. W., & Grant-Muller, S. M. (2015). Appraisal and Evaluation of Interurban ITS : A European Survey. IEEE Transactions on Intelligent Transportation Systems, 16(3), 1070–1087. https ://doi.org/10.1109/TITS.2014.2351253

[151] Lai, C., Zhang, K., Cheng, N., Li, H., & Shen, X. (2017). SIRC : A Secure Incentive Scheme for Reliable Cooperative Downloading in Highway VANETs. IEEE Transactions on Intelligent Transportation Systems, 18(6), 1559–1574. https://doi.org/10.1109/TITS.2016.2612233

[152] Li, Q., Malip, A., Martin, K. M., Ng, S.-L., & Zhang, J. (2012). A Reputation-Based Announcement Scheme for VANETs. IEEE Transactions on Vehicular Technology, 61(9), 4095–4108. https ://doi.org/10.1109/TVT.2012.2209903

[153] Mahmoud, M. E., & Shen, X. (2011). An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Dropping Attack in Multihop Wireless Networks. IEEE Transactions on Vehicular Technology, 60(8), 3947–3962. https ://doi.org/10.1109/TVT.2011.2162972

[154] Otoum, S., Al Ridhawi, I., & Mouftah, H. T. (2020). Blockchain-Supported Federated Learning for Trustworthy Vehicular networks. GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 1–6.https://doi.org/10.1109/GLOBECOM42002.2020.9322159

[155] Oyente. (n.d.). https ://github.com/ethereum/oyente

[156] Posner, J., Tseng, L., Aloqaily, M., & Jararweh, Y. (2021). Federated Learning in Vehicular networks : Opportunities and Solutions. IEEE Network, 35(2), 152–159. https ://doi.org/10.1109/MNET.011.2000430

[157] Solidity. (n.d.). https ://solidity.readthedocs.io/en/develop/

[158] The DAO smart contract. (n.d.) http://etherscan.io/address/%0D%0A0xbb9bc244d798123fde783fcc1c72d3bb8c189413#code

[159] Truffle. (n.d.). https://trufflframework.com/

[160] Vijayakumar, P., Azees, M., Kannan, A., & Jegatha Deborah, L. (2016). Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks. IEEE Transactions on Intelligent Transportation Systems, 17(4), 1015–1028 https://doi.org/10.1109/TITS.2015.2492981

[161] Muhammad Sohail, Zohaib Latif, Shahzeb Javed, Sujit Biswas, Sahar Ajmal, Umer Iqbal, Mohsin Raza, Abd Ullah Khan. *Routing protocols in Vehicular Adhoc Networks (VANETs) : A comprehensive survey. Internet of Things*, 23, 100837, 2023. https://doi.org/10.1016/j.iot.2023.100837

[162] Noora Alromaihi, Alauddin Y. Al-Omary. *Machine Learning and Big Data Based IDS System Extensive Survey.* In : *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 7-12, 2022. 10.1109/3ICT56508.2022.9990066

[163] Sachin Sharma, Piyush Agarwal, Seshadri Mohan. *Security Challenges and Future Aspects of Fifth Generation Vehicular Adhoc Networking (5G-VANET) in Connected Vehicles.* In : *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, 1376-1380, 2020. 10.1109/ICISS49785.2020.9315987

[164] Houda Amari, Lyes Khoukhi, Lamia Hadrich Belguith. *Prediction and detection model for hierarchical Software-Defined Vehicular Network.* In : *2022 IEEE 47th Conference on Local Computer Networks (LCN)*, 463-470, 2022. 10.1109/LCN53696.2022.9843483

[165] Houda Amari, Zakaria Abou El Houda, Lyes Khoukhi, Lamia Hadrich Belguith. *Trust Management in Vehicular Ad-Hoc Networks : Extensive Survey. IEEE Access*, 11, 47659-47680, 2023. 10.1109/ACCESS.2023.3268991

[166] Houda Amari, Wassef Louati, Lyes Khoukhi, Lamia Hadrich Belguith. *Securing Software-Defined Vehicular Network Architecture against DDoS attack.* In : *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, 653-656, 2021. 10.1109/LCN52139.2021.9524953

[167] Houda Amari, Wassef Louati, Lyes Khoukhi, Lamia Hadrich Belguith. *TCP Incast Solutions in Data Center Networks : Survey.* In : *Hybrid Intelligent Systems*, 535-545, 2021. https://doi.org/10.1145/3485730.3493444

[168] Jinyu Zhang, Honghui Zhao, Yumeng Yang, Jiaqi Yan. *Towards Transparency and Trustworthy : A Used-Car Deposit Platform Based on Blockchain.* In : *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 46-50, 2019. 10.1109/QRS-C.2019.00022

[169] Ahmad Mostafa. *VANET Blockchain : A General Framework for Detecting Malicious Vehicles. Journal of Communications*, 2019. 10.12720/jcm.14.5.356-362

[170] Mirador Labrador, Weiyan Hou. *Implementing blockchain technology in the Internet of Vehicle (IoV).* In : *2019 International Conference on Intelligent Computing and its Emerging Applications (ICEA)*, 5-10, 2019. 10.1109/ICEA.2019.8858311

[171] Jaewon Noh, Sangil Jeon, Sunghyun Cho. *Distributed Blockchain-Based Message Authentication Scheme for Connected Vehicles. Electronics*, 9(1), 74, 2020. https://www.mdpi.com/2079-9292/9/1/74

[172] Viraaji Mothukuri, Prachi Khare, Reza M. Parizi, Seyedamin Pouriyeh, Ali Dehghantanha, Gautam Srivastava. *Federated-Learning-Based Anomaly Detection for IoT Security Attacks. IEEE Internet of Things Journal*, 9(4), 2545-2554, 2022. 10.1109/JIOT.2021.3077803

[173] Mohamed Abdel-Basset, Hossam Hawash, Karam Sallam. *Federated Threat-Hunting Approach for Microservice-Based Industrial Cyber-Physical System. IEEE Transactions on Industrial Informatics*, 18(3), 1905-1917, 2022. 10.1109/TII.2021.3091150

[174] Tuo Zhang, Chaoyang He, Tianhao Ma, Lei Gao, Mark Ma, Salman Avestimehr. *Federated Learning for Internet of Things.* In : *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, 413-419, 2021. https://doi.org/10.1145/3485730.3493444

[175] Google. Google Colab. Accessed on september, 2023. https://colab.research.google.com

[176] NSL-KDD dataset. Accessed on september, 2023.https://www.unb.ca/cic/datasets/nsl.html

[177] Fa Xin, Jinghui Zhang, Junzhou Luo, Fang Dong. *Federated Learning Client Selection Mechanism Under System and Data Heterogeneity.* In : *2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 1239-1244, 2022. 10.1109/CSCWD54268.2022.9776061