An Innovative Reputation System for Trustworthy and Secure Vehicle-to-Vehicle Communications

Thesis submitted to the University of Nottingham for the degree of
Doctor of Philosophy, Jan 2025.

Dimah Almani

20318964

Supervised by

Prof. Steven Furnell
Dr. Tim Muller

Signature ____________________

Abstract

Vehicular Ad Hoc Networks (VANETs) are a promising technology that ensures secure and efficient transportation by allowing vehicles to seamlessly communicate with each other and with infrastructure to share real-time information and make better decisions while travelling. However, determining which information is accurate under certain circumstances, such as in the event of an accident, may become challenging when receiving messages from multiple nearby vehicles. Therefore, trusting these messages requires a reliable and secure system to guard against insider attackers, who may intentionally send misleading information, particularly in scenarios without extensive Roadside Units (RSUs) to mediate these exchanges.

Existing standards, such as the Security Credential Management System (SCMS), supply vehicles with pseudonym certificates to meet security and privacy requirements. However, this system has difficulties ensuring that the revoked certificates are updated in regions with limited connectivity access. In order to solve this issue, this research proposes a novel reputation system to maximize the chance of making an accurate decision based on the received messages. This builds upon existing standards and specifications to integrate an innovative Pre-Signature scheme for effective reputation dissemination.

The Pre-Signature scheme enables vehicles to assess dynamically and rely on the most trustworthy information available, even in challenging and limited environments. The research develops realistic simulations of 24-hour rural scenarios to replicate real-time communication challenges. The simulation work also includes accident and malicious attack scenarios, thus giving a wide-ranging performance evaluation of the Pre-Signature scheme under typical infrastructural constraints. The results revealed a significant enhancement in decision-making accuracy with conflicting information, achieving an improvement ranging from 36% in *Accidents* and 44.4% in *No-Accident* scenarios in a rural environment compared to the existing certification system.

Finally, a new reporting scheme, Distributed Reputation for Accurate Vehicle Misbehaviour Reporting (DRAMBR), is proposed to improve reporting efficiency in disconnected areas by effectively mitigating false reports while distinguishing between honest reporters, system errors and malicious behaviours. Experimental results indicate that the DRAMBR system achieves 98% effectiveness in distinguishing between behaviours, highlighting its overall performance.

The contribution of the thesis is related to the development of VANETs, in particular, to improve the reliability and efficiency of V2V communications in critical areas, enabling safer, more secure, and efficient transport networks.

Dedication

I dedicate this work to the memory of my late father, Mohammed, whose legacy of integrity, and wisdom continues to inspire me. Although he is no longer here to witness this milestone, his spirit has been a constant source of strength.

To my great mother, Munira, nothing would have been possible without you. From the very first steps, your depth of love, encouragement, and wise counsel have been invaluable to me in this work and life. Your sacrifices are woven into every word of this thesis. Every challenge and every triumph is a reflection of your love and unwavering support. I hope this achievement makes you as proud of me as I am to be your child.

To my beloved husband, Dr.Abdulaziz, your unwavering love and support have been my guiding lights when the path seemed daunting. Thank you for standing by my side through every challenge, believing in me when I doubted myself , and celebrating every step in my progress. I can never be thankful enough for the sacrifices you went through to bring me to this moment. I'm truly blessed sharing this life and journey with you.

To my wonderful children, my little superhero, Abdulrahman, and my little princess, Munirah, you are my greatest motivation and joy. Your giggles, cuddles and love were my greatest source of strength and inspiration throughout this journey. Every late night and every challenge I faced was worth it, knowing it was for a future that will make you proud. I hope this work inspires you to follow your dreams with passion and determination.

Acknowledgements

PhD is the outcome of the cooperation and support of several people both at professional and personal levels. I would like to acknowledge all the people who helped me to achieve my goal.

First and foremost, I extend my sincere thanks to my supervisors, whose unwavering support and invaluable insights have been instrumental in shaping this work. I will always feel proud to be their first PhD student and the first PhD completion from the Cyber Security group at the University of Nottingham. I would like to thank my main supervisor, Prof. Steven Furnell for providing me an excellent opportunity to work under his guidance. This journey wouldn't be possible without his extensive support and encouragement. His dedication and encouragement empowered me to push boundaries, and his guidance has profoundly impacted both my research and personal academic growth. I also had the privilege of working with my second supervisor, Dr. Tim Muller, his research experience helped me greatly in this thesis, and the fruitful discussions with him will remain unforgettable. His willingness to share knowledge and offer constructive advice is deeply appreciated. I would also like to express my gratitude to Dr.Xavier Carpent, his collaboration and thoughtful feedback have played an important role in shaping my research

To my brothers, Ayman and Abdulrahman, our bond has inspired and motivated me throughout my life. You have been my role models and my biggest cheerleaders. This thesis is dedicated to you both for inspiring me to dream big and work hard every step of the way, and I hope it makes you as proud of me as I am to have you as my brothers. Equally important is the appreciation expressed to my colleagues at the CybSec group, for all the moments spent supporting each other with caring, laughter, and enlightenment. Lastly, to my extended family and friends, thank you for your love and constant encouragement. This journey has been made easier by your presence, and I am fortunate to have you all in my life.

List of Publications

The following is a chronological list of papers produced and published during the conduct of the research. These are referred to as appropriate within the main body of the thesis using the designator Publication n.[1]

1. **Supporting Situational Awareness in VANET Attack Scenarios** [Published]

   Dimah Almani, Steven Furnell, and Tim Muller

   European Conference on Cyber Warfare and Security (ECCWS), 2022.

2. **Assessing the Impact of Attacks on Connected and Autonomous Vehicles in Vehicular Ad Hoc Networks** [Published]

   Kaushik Balaji, Dimah Almani, and Steven Furnell

   9th International Conference on Information Systems Security and Privacy (ICISSP), 2023.

3. **A Pre-Signature Scheme for Trustworthy Offline V2V Communication** [Published]

   Dimah Almani, Tim Muller, Steven Furnell, Xavier Carpent and Takahito Yoshizawa

   Proceedings of the 14th IFIP International Conference on Trust Management (IFIPTM), 2023.

4. **Enabling Vehicle-to-Vehicle Trust in Rural Areas: An Evaluation of a Pre-Signature Scheme for Infrastructure-Limited Environments** [Published]

   Dimah Almani, Tim Muller, Steven Furnell, Xavier Carpent and Takahito Yoshizawa

   Selected as the ***Cover Story*** *Future Internet (MDPI), 2024.*

[1] corresponds to the sequence of the publication.

5. **Reputation Mechanism Simulations for V2V Communication in Limited Infrastructure Scenarios** [Published]

   Dimah Almani, Steven Furnell, and Tim Muller

   19th International Conference for Internet Technology and Secured Transactions, (ICITST), 2024.

6. **Leveraging Reputation for Enhanced Decision Accuracy in Vehicle-to-Vehicle communications under Limited Infrastructure** [Published]

   Dimah Almani, Tim Muller, and Steven Furnell

   Vehicular Communications (Springer), 2025.

7. **Distributed Reputation Mechanism for Accurate Vehicle Misbehaviour Reporting (DRAMBR)** [Published]

   Dimah Almani, Tim Muller, and Steven Furnell

   Future Internet (MDPI), 2025.

Table of Contents

Abstract ii

Dedication iii

Acknowledgements iv

List of Publications v

List of Tables xii

List of Figures xiv

Abbreviations xix

Chapter 1 Introduction 1

1.1 Research Context 2

1.2 Motivation 6

1.3 Aim and Objectives 7

1.4 Contributions 8

1.5 Thesis Organisation 11

Chapter 2 Theoretical Foundations of Vehicular Networks 16

2.1 Introduction 17

2.2 Core Concepts of VANETs 17

2.2.1 VANET Architecture 19

2.2.2 Main Components of VANETs 22

2.2.3 Levels of Automation in VANETs 26

2.3 Message Exchange in Vehicular Networks 29

2.3.1 Communication Protocols in V2V 29

2.3.2 Dedicated Short-Range Communication 31
2.3.3 Safety Messages in V2V Communications 34
2.4 Disconnected Areas of Vehicular Networks 38
2.4.1 Characteristics of Disconnected Areas 39
2.4.2 Case Study of Disconnected Areas 41
2.4.3 Mitigation Strategies for Disconnected Areas 43
2.5 Conclusion 44
Chapter 3 Security Paradigms and Challenges in V2V Networks 45
3.1 Introduction 46
3.2 Security Threats and Attacks 46
3.2.1 Security Attacks Analysis 47
3.2.2 Potential Attacks Scenarios 53
3.3 Security Requirements and Challenges 57
3.3.1 Security Requirements 57
3.3.2 Security Challenges 60
3.4 SCMS Role in Vehicular Networks 62
3.4.1 SCMS Architecture Overview 64
3.4.2 SCMS: Pseudonym Certificates 70
3.4.3 Misbehaviour Detection and Revocation 71
3.4.4 SCMS Limitation with Disconnectivity 74
3.5 Conclusion 76
Chapter 4 Security, Privacy, and Trust in V2V Networks 77
4.1 Introduction 78
4.2 V2V Studies in Disconnected Areas 78
4.2.1 V2V Connectivity in Rural Areas 79
4.2.2 RSU Deployment in Rural Areas 81
4.3 Analysis of Certificate Management 84
4.3.1 Public Key Infrastructure (PKI) 84

4.3.2 Digital Certificates and Signatures 87

4.4 Trust and Reputation in Vehicular Networks 89

4.4.1 Evaluating Trust Mechanisms 89

4.4.2 Exploration of Reputation Systems 96

4.5 Discussion: Reputation via Privacy, Security, and Trust . . . 101

4.6 Conclusion 106

Chapter 5 A Pre-Signature Scheme for Enabling Vehicle-to-Vehicle Trust in Rural Areas 107

5.1 Introduction 108

5.2 Proposed System Framework 110

5.2.1 Framework Entities 110

5.2.2 V-PKI Architecture with RS 112

5.3 Novel Signature Scheme 117

5.4 Reputation Decay Mechanism 121

5.4.1 Reputation Value 122

5.5 Privacy-Preserving V2V Communication 124

5.5.1 Vehicular Communication 124

5.5.2 Vehicle Privacy 126

5.6 Operational Considerations 127

5.6.1 RS to Vehicle 127

5.6.2 V2V Communication 127

5.6.3 Computation Overhead 128

5.7 Establishing the Simulation Environment 129

5.7.1 Simulation Concept Overview 129

5.7.2 Selection of the Simulation Tool 130

5.7.3 RSU Placement Using Voronoi Diagrams 131

5.7.4 Experimental Setup 132

5.8 Simulation Results Discussion 135

5.8.1 Key Metrics Analysed 137

5.8.2 Evaluating RSU Availability and Overnight Connectivity . . . 138
5.8.3 Results Synthesis: Pre-Signature Scheme in Rural Vehicular Communication Areas . . . 147
5.9 Conclusion . . . 148
Chapter 6 Reputation-Based Decision Accuracy in V2V Communication with Limited Infrastructure 149
6.1 Introduction . . . 150
6.2 System Model . . . 151
6.2.1 Operational Behaviour of Vehicles . . . 151
6.2.2 Proposed System . . . 156
6.2.3 Distribution of Reputation Values . . . 159
6.2.4 Reputation System Procedures . . . 161
6.3 Simulation Design . . . 164
6.3.1 Simulation Tools Integration . . . 164
6.3.2 Simulation Scenarios . . . 167
6.3.3 Experimental Setup . . . 171
6.4 Results : Performance Analysis and Evaluation . . . 174
6.4.1 Evaluating The Effectiveness of CRA and CRNA Over CCA and CCNA . . . 176
6.4.2 CRV and CPC Performance: Precision, Recall, and F-Score Analysis . . . 181
6.4.3 CRA and CRNA Impact on Decision Accuracy . . . 183
6.5 Conclusion . . . 184
Chapter 7 Distributed Reputation for Accurate Vehicle Misbehaviour Reporting (DRAMBR) 185
7.1 Introduction . . . 186
7.2 DRAMBR System Model . . . 188
7.2.1 DRAMBR Assumptions . . . 189

7.2.2 Vehicle Behaviour in OE and OR 190

7.2.3 DRAMBR Framework 192

7.2.4 Workflow and DRAMBR Phases 194

7.3 DRAMBR Technical Implementation 206

7.3.1 DRAMBR: Offline Evaluation 206

7.3.2 DRAMBR: Online Reporting 207

7.4 DRAMBR Experimental Evaluation 217

7.4.1 Experiment Description 217

7.4.2 Simulation Setup 218

7.5 Results and Discussion 221

7.5.1 Results From Applying DBSCAN 222

7.5.2 Results From Applying Isolation Forest 225

7.5.3 Gaussian Mixture Model (GMM) 227

7.5.4 DRAMBR Accuracy 228

7.6 Conclusion 231

Chapter 8 Conclusions and Future Research 232

8.1 Summary of Achievements 233

8.2 Limitations of The Research 235

8.3 Directions for Future Work 238

8.4 Enabling Trust in Offline V2V Networks 240

References 241

Appendices 266

Appendix A Preliminary Simulation Study 267

Appendix B Simulation Overview and Examples 274

Appendix C Source Code and Simulation Data 278

List of Tables

2.1 Outlining the Main Components of a VANET. 23

2.2 Outlining the Key Components of OBUs. 25

2.3 SAE Automation Levels. 27

2.4 Main Communication Protocols in V2V. 30

2.5 Types of Safety Messages in VANETs. 35

2.6 Connectivity Mitigation Strategies for Disconnected Areas. . 44

3.1 Comparison of Security Attacks in VANETs 48

4.1 Trust Features in Vehicular Networks. 91

4.2 Trust Entities in Vehicular Networks. 92

4.3 Three Main Factors of the Trust System. 94

4.4 Limitations in the Existing Reputation Schemes. 101

5.1 Simulation Parameters. 133

6.1 System Notations and Definitions 161

6.2 Summary of Examined Scenarios and Communications. . . . 168

6.3 Simulation Parameters. 171

7.1 DRAMBR System Units. 194

7.2 Rep_{Veh} Observing Misbehaviour Action. 195

7.3 Rep_{Vehs} Reporting Conditions and RS Actions. 200

7.4 MR_f Classification. 203

7.5 Actions Triggered by the RS for Tar_{Veh} and Rep_{Veh} 204

7.6 Accident Scenarios and Triggered Misbehaviour Reports (MRs)218

7.7 DRAMBR Simulation Details. 220

7.8 DRAMBR Pipeline. 221

7.9 Performance Accuracy Across Scenarios 230

List of Figures

1.1 Coverage Map of the Peak District Area. 3

1.2 An Integrated Approach for Reputation, Offline Operation, and Privacy in V2V. 5

1.3 Thesis Organisation. 15

2.1 Types of Communications in IoV Network. 18

2.2 VANET Communications Architecture. 19

2.3 OBUs in Autonomous Vehicle. 24

2.4 SAE Levels of Automation. 26

2.5 Frequency and Channel Division of DSRC. 32

2.6 DSRC Protocol Stack. 33

2.7 Structure of the DENM Message Part I; Part II. 37

2.8 Message-Format-of-WAVE-Short-Message-WSM. 37

2.9 Peak District Map Extracted from OpenStreetMap (OSM). . 41

2.10 Peak District Environment Extracted from Google Map. . . 42

3.1 Taxonomy of Security Attacks Targeting Services in VANETs. 49

3.2 Scenarios of Vulnerability to Malicious Attacks in VANETs. 55

3.3 SCMS Architecture Design. 65

3.4 Challenges of SCMS in Disconnected Vehicular Network. . . 75

4.1 Taxonomy of RSU deployment. 82

4.2 Strategic RSU Deployment Map for Optimal Coverage in a 10 km^2 Area of the Peak District. 83

4.3 Security-Aware Routing Method VANSec. 94

4.4 Trust Establishment Process. 95

4.5 Relationship Between Privacy, Security, and Trust in V2V Communications. 102

5.1 Proposed System Framework. 111

5.2 V-PKI Architecture with RS. 113

5.3 RV Retrieval. 114

5.4 DENM Message Handling. 116

5.5 Sequence Diagram for Typical Operation of a Pre-Signature Scheme. 119

5.6 Decay of Reputation Over Time 123

5.7 The Structure of a DENM Message. 124

5.8 Emergency V2V Communication Scenario. 126

5.9 DENM Message Signed by*Pre-Signature*. 128

5.10 SUMO Architecture: Simulation Processes. 131

5.11 V2R Communication for Updating RV and Obtaining *Pre-Signature* from RSU. 136

5.12 V2V Reputable Communication: Within RSU Range. 136

5.13 Offline V2V Reputable Communication: Outside RSU Range.136

5.14 Vehicle Communication Activity Over Time with Limited Connectivity. 138

5.15 Time-Based Analysis of Communications Metrics for RSU 1 with 0% Overnight Connectivity. 139

5.16 Analysis of Vehicular Communication Efficacy under 30% Overnight Connectivity Across Various RSU Densities, with Comparisons at 300 m Range **(Left)** and 900 m Range **(Right)**. 142

5.17 Analysis of Vehicular Communication Efficacy under 50% Overnight Connectivity Across Various RSU Densities, with Comparisons at 300 m Range **(Left)** and 900 m Range **(Right)**. 142

5.18 Analysis of Vehicular Communication Efficacy under 70% Overnight Connectivity Across Various RSU Densities, with Comparisons at 300 m Range **(Left)** and 900 m Range **(Right)**. 142

5.19 Analysis of Communication Types over Overnight Percentage in High RSU Range = 900 m for 1 RSU (**Left**) and 3 RSUs (**Right**). 145

5.20 Analysis of Communication Types over Overnight Percentage in Low RSU Range = 300 m for 5 RSUs (**Left**) and 10 RSUs (**Right**). 146

6.1 Illustration of Sybil Attack Threat Scenario. 152

6.2 Phased Approach to Message Verification and Decision Making. 157

6.3 Integration of Simulation Tools. 165

6.4 Triangle Distribution of the RVs. 166

6.5 Target Area of Peak District Segment in OMNeT++. 168

6.6 Screenshots comparing accident scenarios across communications using the (a) Certificate-based System and (b) Reputation-based System. 175

6.7 Comparison of **TP** Rates Across Vehicles in Accident Scenario **(Top)** and No Accident Scenario **(Bottom)**. 177

6.8 Comparison of **TN** Rates Across Vehicles in Accident Scenario **(Top)** and No Accident Scenario **(Bottom)**. 178

6.9 Comparison of **FP** Rates Across Vehicles in Accident Scenario **(Top)** and No Accident Scenario **(Bottom)**. 179

6.10 Comparison of **FN** Rates Across Vehicles in Accident Scenario **(Top)** and No Accident Scenario **(Bottom)**. 180

6.11 Performance of CCA, CRA (Top), CRNA, and CCNA (Bottom): Precision, Recall, and F-score. 182

6.12 CRA and CRNA Impact on Decision Accuracy. 183

7.1 False M_{sg} / MR_f Causes. 191

7.2 MR Attack. 191

7.3 Proposed Misbehaviour Reporting System (DRAMBR). . . . 193

7.4 Local Misbehaviour Detection Mechanism (LMDM). 196

7.5 Process 2: Online Reporting Illustration. 202

7.6 MR Evaluation. 207

7.7 Illustration of DBSCAN. 210

7.8 Simulated Map of Peak District Area. 219

7.9 DBSCAN Clustering Results for Different Scenarios: $ACD-OCC$, $ACD-ABS$, $ACD-RSL$. 223

7.10 Isolation Forest Results on DBSCAN Noise Points. 226

7.11 Reporter Classification Results. 227

7.12 Confusion Matrix Representing DRAMBR Performance in Noise-Based Accuracy. 229

7.13 Confusion Matrix Representing DRAMBR Performance in $ACD{-}OCC$ (**Left**), $ACD{-}ABS$(**Middle**), $ACD{-}RSL$(**Right**).229

7.14 Accuracy, Precision, Recall, and F1-Score Across Scenarios and Overall System 230

Abbreviations

ADAS Advanced Driver Assistance System.

AODV Ad hoc OnDemand Distance Vector.

AVs Autonomous Vehicles.

BSM Basic Safety Messages.

CA Certification Authority.

CAVs Connected and Autonomous Vehicles.

CCA Communication using Certificates during Accident.

CCNA Communication using Certificates with No Accident.

CRA Communication using Reputation during Accident.

CRL Certification Revocation List.

CRNA Communication using Reputation with No Accident.

DBSCAN Density Based Spatial Clustering of Applications with Noise.

DENM Decentralised Environmental Notification Message.

DRAMBR Distributed Reputation for Accurate MisBehaviour Reporting.

DSDV Destination-Sequenced Distance Vector.

DSRC Dedicated Short-Range Communication.

ECDSA Elliptic Curve Digital Signature Algorithm.

ETSI European Telecommunications Standards Institute.

GMM Gaussian Mixture Model.

GSM Global System for Mobile communications.

IoV Internet of Vehicles.

ITS Intelligent Transport Systems.

LMDM Local Misbehaviour Detection Mechanism.

MA Misbehaviour Authority.

MAC Medium Access Control.

MR Misbehaviour Report.

OBUs On-Board Units.

OMNeT++ Objective Modular Network Testbed in C++.

PCA Pseudonym Certificate Authority.

PCs Pseudonym Certificates.

QoS Quality of Service.

RA Registration Authority.

RS Reputation Server.

RSUs Roadside Units.

RV Reputation Value.

SCMS Security Credential Management System.

SUMO Simulation of Urban Mobility.

TA Trusted Authority.

Veins Vehicles in Network Simulation.

V-PKI Vehicular Public Key Infrastructure.

V2I Vehicle-to-Infrastructure.

V2V Vehicle-to-Vehicle.

VANETs Vehicular Ad-hoc Networks.

WAVE Wireless Access in Vehicular Environments.

WSM WAVE Short Message.

Chapter 1

Introduction

The introduction chapter establishes the foundation for the research and sets the stage for understanding the study context and the research gap. It highlights the importance of the investigation by presenting the motivation behind it, leading to a clear articulation of the research's main aim and objectives, along with the related research questions. Additionally, this chapter briefly explains the study's contribution and outlines the structure of the remaining chapters.

1.1 Research Context

Vehicular Ad-hoc Networks (VANETs) are promising technologies that ensure secure and efficient transportation by allowing vehicles to communicate and share critical information like location and road conditions to alert each other, particularly through Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. Infrastructure such as Roadside Units (RSUs) is employed to confirm the source validity of such information before the vehicles act upon it, which facilitates the validation of the source's credentials and ensures a trustworthy communication process. Nonetheless, further validation is required in rural areas with limited infrastructure and low connectivity. While cellular communication technologies are undoubtedly widespread, they are not universally accessible, due to geographic limitations. For example, an examination of the GSMA website[1] (GSMA, 2025) clearly illustrates that the coverage in some areas is not always guaranteed, and it is easy to find many places in different countries where there is road infrastructure, yet 2G coverage is lacking (let alone coverage from 3G or higher networks).

The Peak District, a National Park in central England, has identified coverage gaps. As shown in Figure 1.1, the red areas represent regions with cellular coverage, whereas the green areas indicate those without. For instance, road A57 is located in an area lacking cellular coverage. In these situations, vehicles solely rely on neighbouring vehicles for communication forming a V2V network rather than a centralised network. This reliance makes the authentication of the received messages crucial for ensuring reliable V2V communication (Harshit et al., 2025). In this case, the effectiveness of the communications is critically undermined by the challenge of ensuring the integrity of the information exchanged, particularly

[1] https://www.gsma.com/coverage/

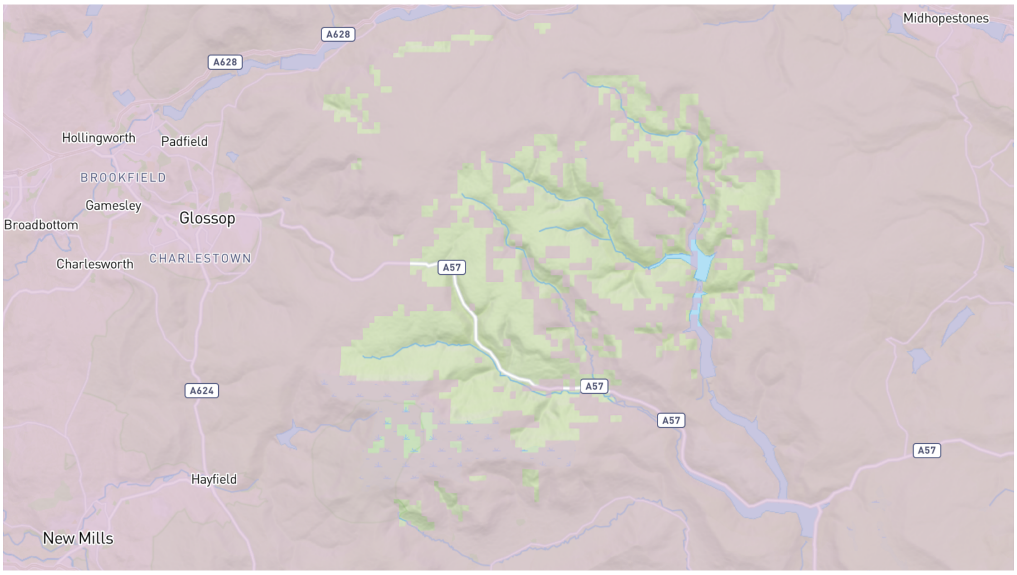


Figure 1.1: Coverage Map of the Peak District Area.
Source: GSMA

in scenarios laden with conflicting messages and in the absence of extensive RSUs to mediate these exchanges. Such circumstances require reliable communication methods to ensure trust between vehicles.

An analysis of the existing literature has identified various studies proposing solutions to ensure secure communication under ideal VANETs conditions. However, addressing the issue of V2V communication during emergencies in disconnected environments remains unresolved. One must recognise that a recent and significant portion of these investigations discuss the traditional cryptography standards like the Vehicular Public Key Infrastructure (V-PKI), where vehicles utilise certificates and signatures to authenticate the information source and ensure security up to a certain level within the network. A prime model of this can be seen in the implementation of the Security Credential Management System (SCMS) which supplies vehicles with certificates to meet the security and privacy requirements (Brecht et al., 2018). However, sole dependence on such a standard is insufficient during the verification process in areas with limited connectivity due to some complications, such as ensuring certificates are up-to-date.

Building on previous work in the domain of certificate-based security measures and reputation-based trust models, this research contributes by providing further insight into how trust can dynamically be established in a disconnected environment. It targets the role of reputation mechanisms in enhancing communication accuracy and reliability by filtering false message attacks and mitigating misbehaviour in scenarios where vehicles are unable to verify messages through conventional online security mechanisms.

The research further extends the literature by introducing an innovative cryptographic primitive, the Pre- Signature, that involves a new entity Reputation Server (RS) and integrating it with the SCMS, proposing a novel framework, ensuring that communication remains secure and reliable, even without continuous online connectivity. The unique ability of the scheme to incorporate the Reputation Value (RV) with the Pseudonym Certificates (PCs) and append them to each transmitted message that is subsequently authenticated using cryptographic methods, establishing a privacy-friendly decentralised trust mechanism in the absence of RSUs for secure offline communication.

The research emphasises the importance of balancing privacy, security, and trust to establish robust and secure V2V communication in offline settings. Referring to Figure 1.2, the combination of Reputation and Offline can be delivered by foregoing pseudonyms and providing medium-term (e.g., daily) Reputation Value certificates. Meanwhile, Reputation and Privacy can be delivered by requesting a short-term RV certificate every time a new Pseudonym Certificate is used. Finally, Privacy and Offline is delivered by systems like SCMS. The challenge is to deliver all three of these properties in a scalable way, with minimal changes to the standards.

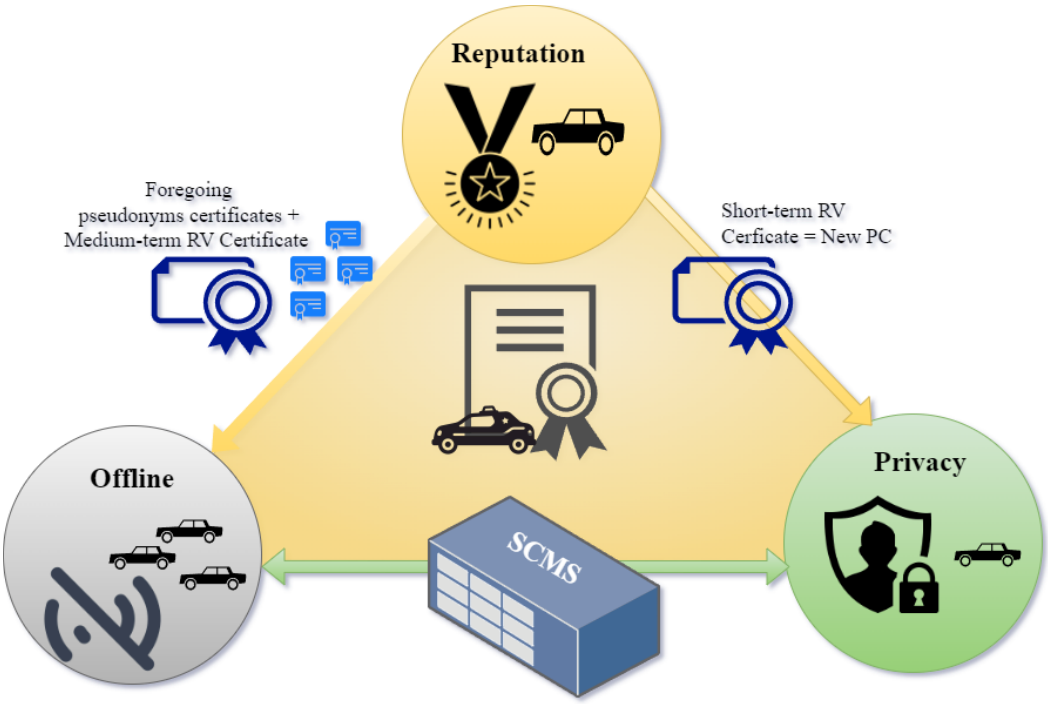


Figure 1.2: An Integrated Approach for Reputation, Offline Operation, and Privacy in V2V.

A significant aspect of this research is to simulate extensive communication scenarios under various conditions to compare the existing SCMS certificates-based system with the proposed enhancement, which incorporates reputation features into the current standard. The aim is to measure the impact of the reputation system on rural regions with a limited density of RSUs. The Peak District provides a suitable case study as it is characterised by high levels of disconnected areas and low infrastructure density, both critical difficulties that the work can investigate solutions to address.

The research results validate that the reputation-based system supported by the *Pre-Signature* authentication scheme, significantly improves the decision accuracy within V2V communications in the constrained conditions of rural environments. The study represents a theoretical contribution to the improvement of V2V communication systems since it places into perspective one of the critical points: reputation-based trust mechanisms versus mechanisms that rely solely on cryptographic authentication. It also offers practical solutions and insights to address the information reliability challenges encountered in areas with limited infrastructure. The simulation studies highlight the proposed approach's capability of enabling vehicles to make intelligent and safe decisions that promote the overarching objective of enhancing road safety and efficiency in rural settings.

1.2 Motivation

The Internet of Vehicles (IoV) evolves towards ever-higher levels of vehicle autonomy. As a result, the reliance on Autonomous Vehicles (AVs) technology has experienced rapid growth in recent years. This technology allows users to share crucial safety information such as road conditions, hazards, and traffic. However, rural areas face challenges due to limited infrastructure and intermittent connectivity, undermining the trust and security of V2V communication, especially during emergencies.

Without continuous connectivity in such areas, vehicles are unable to authenticate both the receiving messages as well the legitimacy of the sender. This situation makes communication vulnerable to various attacks, which could endanger drivers and vehicles as a result. Thus, this research is motivated by the need to protect users against possible risks caused by untrustworthy or malicious vehicles, especially in disconnected environments, to safeguard the passengers and the network.

1.3 Aim and Objectives

The research aims to design, develop and evaluate a novel reputation system for trustworthy V2V communication in disconnected areas, enhancing message validation and mitigating malicious activities under emergencies without requiring continuous online connectivity. To achieve this overarching aim, five research objectives have been established (each of which is also framed as an associated research question).

- **Objective 1: To investigate and understand the vulnerabilities of V2V communications in disconnected areas.**

  This objective aims to answer **RQ1**: How can the trustworthiness of V2V communication in disconnected areas be effectively fortified under different attack scenarios? *Chapters 2 and 3* address this objective through a detailed analysis of the corresponding RQ.

- **Objective 2: To design a novel framework that integrates a Reputation Server (RS) with the SCMS.**

  This objective answers **RQ2**: How can the fusion of reputation management with pseudonym privacy contribute to a paradigm shift in enhancing the dependability and integrity of V2V communication in disconnected areas? *Chapter 4* provides an analysis and discussion that lays the groundwork for the main framework and addresses this objective and its associated RQ.

- **Objective 3: To introduce a signature scheme that enables vehicles to verify their reputations in a secure and private manner without dependence on continuous connectivity.**

This objective answers **RQ3**: How can reputation and pseudonymity be balanced appropriately, ensuring trustworthy offline V2V communication without compromising security and privacy standards? *Chapter 5* introduces a novel scheme that addresses this objective and its associated RQ.

- **Objective 4: To evaluate the impact of reputation on decision-making accuracy during adversarial scenarios and under emergencies.**

  This objective answers **RQ4**: How can reputation mitigate the risks of misleading information generated by malicious in environments with intermittent connectivity? The RQ4 tied to this objective is thoroughly examined in *Chapter 6* through extensive simulation scenarios under different accident conditions.

- **Objective 5: To develop an accurate and efficient reputation-based reporting scheme that leverages the vehicle's feedback to evaluate peer trust dynamically.**

  This objective aims to answer **RQ5**: How can reputation facilitate the feedback process and mitigate the risks of dishonest feedback? *Chapter 7* explores this objective and its related RQ through a detailed, multi-layered novel scheme designed to accurately detect and classify misbehaviours in V2V networks.

1.4 Contributions

The research proposes various novel contributions utilising reputation to enrich trust management in vehicular networks. The main contribution is to develop a reputation scheme that operates efficiently in disconnected rural areas for more reliable and trustworthy V2V communications.

The core analytical approach adopted in this study involves designing extensive simulation scenarios under different setups. Using Vehicular network simulation tools: Simulation of Urban Mobility (SUMO), Objective Modular Network Testbed in C++ (OMNeT++), and Vehicles in Network Simulation (Veins), the research conducted various experiments to analyse V2V communication under various emergency and attack scenarios. This analysis further supports the effectiveness of the proposed reputation system in enhancing decision accuracy. The key contributions of this research are classified as follows:

- Integrating the SCMS with a reputation system is proposed to create a novel reputation signature scheme. The novel solution is a two-step signature scheme variant called a Pre-Signature. This scheme enables an appropriate balance between reputation and pseudonymity in offline V2V communication. The Pre-Signature allows reputation to be used even when vehicles are pseudonymous and without access to infrastructure, resulting in improved effectiveness of offline V2V communication.

  Published in: Proceedings of the 14th IFIP International Conference on Trust Management (IFIPTM, 2023) (*Publication 3*).

- The Pre-Signature scheme performance is evaluated in-depth under the typical infrastructural limitations encountered in rural scenarios. The evaluation addresses the unique challenges posed by sparse or irregular Roadside Units (RSUs) coverage in these areas. The study analyses the relationships between three variables: communication range, amount of RSUs, and degree of home-to-vehicle connectivity overnight. The study creates and simulates a 24-hour real-world rural scenario utilising the widely used Simulation of Urban Mobility (SUMO) traffic simulation tool.

The simulation investigates how areas with low RSUs adoption (typically in rural areas) benefit from our Pre-Signature approach.

Published and Selected as the cover article in: Journal of Future Internet (MDPI, 2024) (*Publication 4*).

- A comprehensive comparison study has been conducted to evaluate the efficiency of the reputation in enhancing decision accuracy during emergencies and in the presence of various malicious activities. This study incorporates the Pre-Signature scheme designed to offer reputation values offline. Through different simulation setups, including accident and no-accident scenarios, the study assesses the security performance of the proposed reputation scheme compared to the traditional SCMS, which relies solely on Certification Revocation List (CRL) to block malicious vehicles.

  This preliminary version of the concept and initial simulation procedure was *Published in: 19th International Conference for Internet Technology and Secured Transactions (ICITST, 2024)* (*Publication 5*). (see Appendix A for details). The primary study, which includes further analyses and the final results, has been *Published in the Vehicular communications (Elsevier, 2025)* (*Publication 6*).

- A novel Distributed Reputation for Accurate Misbehaviour Reporting (DRAMBR) is presented. Through its two phases, the proposed DRAMBR has effectively identified and mitigated misbehaviour by leveraging local observations and neighbouring feedback in offline settings. Later, upon connectivity, reports are consolidated with the Reputation Server (RS) to classify these reports accurately. Integrating advanced classification techniques like DBSCAN, Isolated Forest, and XGBoost, DRAMBR effectively distinguishes between honest, malicious, and erroneous reporters.

This ultimately contributes to the reliability and resilience of vehicular communication systems in challenging offline scenarios and assigns reputation more accurately to both the reporters and the targeted vehicles. The primary study has been *Published in the Future Internet (MDPI, 2025)* (*Publication 7*).

The complete source code and related simulation data used in this thesis are provided in (*Appendix C*) for reference and reproducibility purposes.

- A further paper, entitled ”Assessing the Impact of Attacks on Connected and Autonomous Vehicles in Vehicular Ad Hoc Networks”, has also been published (*Publication 2*). However, it is not included in this thesis as it is based on work conducted by a Master’s student under my supervision, and so was aligned to the PhD research rather than forming a direct contribution to it.

1.5 Thesis Organisation

The remainder of the thesis is organised into seven further chapters as follows:

- **Chapter 2. Theoretical Foundations of Vehicular Networks:** This chapter explains the basic concepts that form the foundation of this research. It begins with an overview of Vehicular Ad-hoc Networks (VANETs) from architecture, main units, and automation levels. It then explores the prevalent message types, shedding light on the protocols for exchanging these messages. In addition, this chapter delves into the challenges presented by regions lacking proper infrastructure, emphasizing the difficulties encountered and highlighting the consequences of such a challenge in V2V communication.

- **Chapter 3. Security Paradigms and Challenges in V2V Networks:** This chapter first overviews various attacks that target the security requirements in VANETs, highlighting potential attack scenarios that may arise in regions with limited network coverage. The discussion emphasises the users' responsibilities and roles in mitigating the risk of such attacks. These perspectives are grounded in the research outcomes of (*Publication 1*). Furthermore, this chapter overviews the key security requirements and explores their challenges. Lastly, the chapter introduces the architecture and the main processes in the standard Vehicular Public Key Infrastructure (V-PKI), the SCMS that utilises certificates to facilitate data transmission between vehicles for more secure and authenticated communications.

- **Chapter 4. Critical Analysis of Contemporary Studies in V2V Communications:** This chapter overviews the work and literature on V2V communication and reputation management systems. The discussion focuses on reviewing the limitations already identified in the related systems. The aim is to systematically analyse and present a thorough evaluation of the critical methodological concepts of reputation systems in V2V communications. The evaluation encompasses various aspects, including reputation system implementation, model evaluation, and SCMS. The chapter culminates in a concise summary of the strengths and weaknesses of existing approaches in this domain. Lastly, this chapter sets the stage for the main system framework by discussing the relationship between privacy, security, and trust requirements and their corresponding solutions within vehicular networks.

- **Chapter 5. A Pre-Signature Scheme for Enabling Vehicle-to-Vehicle Trust in Rural Areas:** This chapter presents an in-depth exploration of the novel reputation system based on the Pre-Signature scheme. It firstly explains the framework and how it aims to seamlessly integrate the reputation server with the SCMS. Next, it introduces a definition and description of the Pre-Signature scheme, highlighting its efficiency in authenticating messages in offline settings. This is followed by a discussion of the scheme's operational considerations. Finally, the related simulation results are presented at the end of the chapter. This chapter is supported by two major papers: the first (*Publication 3*) introduces the Pre-Signature scheme to enable secure V2V communications, while the second (*Publication 4)* uses simulations to assess its performance in rural areas.

- **Chapter 6. Reputation-Based Decision Accuracy in infrastructreless V2V Communications:** This chapter evaluates the integration of the reputation system into the existing certification system to enhance decision accuracy during emergencies in rural areas. By adopting the Pre-Signature scheme, vehicles dynamically assess and rely on the most trustworthy information available, even in an infrastructure-limited environment. The chapter firstly introduces the system model, highlighting the specific threat triggered by the Sybil attack.Next, the chapter describes the experiment design, which compares the security performance of the proposed reputation system with existing communication system certificates. The results are achieved by integrating vehicular simulation tools like SUMO, OMNeT++, and Veins, to evaluate the V2V communications in each system under two conditions (Accident and No accident) ensuring a comprehensive system evaluation.

This chapter draws on two key papers: the first (*Publication 5*) provides the initial idea of the simulation, and the second (*Publication 6*) is the leading study driving the current methodology.

- **Chapter 7. Distributed Reputation Mechanism for Accurate Misbehaviour Reporting in Rural Networks (DRAMBR):** Building on the previous chapter, this chapter finalizes the study by presenting a novel reputation-based reporting approach. The chapter first explains the DRAMBR system, highlighting the vehicles' behaviours in offline and online settings to illustrate the activity of a false reporting attack. Then, DRAMBR's two phases are comprehensively explained, from misbehaviour identification to report submission. The chapter next presents the technical implementation integrating techniques such as DBSCAN and Isolation Forest. This leads to the experiment design, which uses these techniques to distinguish between honest, erroneous , and malicious reporting in three scenarios: Accident, No-Accident, and Accident Resolved. These perspectives are grounded in the research outcomes of (*Publication 7*).

- **Chapter 8. Conclusion and Future Work:** This chapter summarises the overall achievements, findings, and key contributions. Firstly, it synthesizes the study's outcomes to highlight the implications and interconnections observed across the reflecting on its impact in the field of ITS. Following this, the chapter identifies the research limitations and suggests potential directions for future research that could further advance the field with new ideas and innovations.

Figure 1.3 provides a visual representation flow of the chapters within this thesis. The main chapters are also supported by a number of related Appendices (A,B) which are individually referenced at appropriate points within the main discussion.

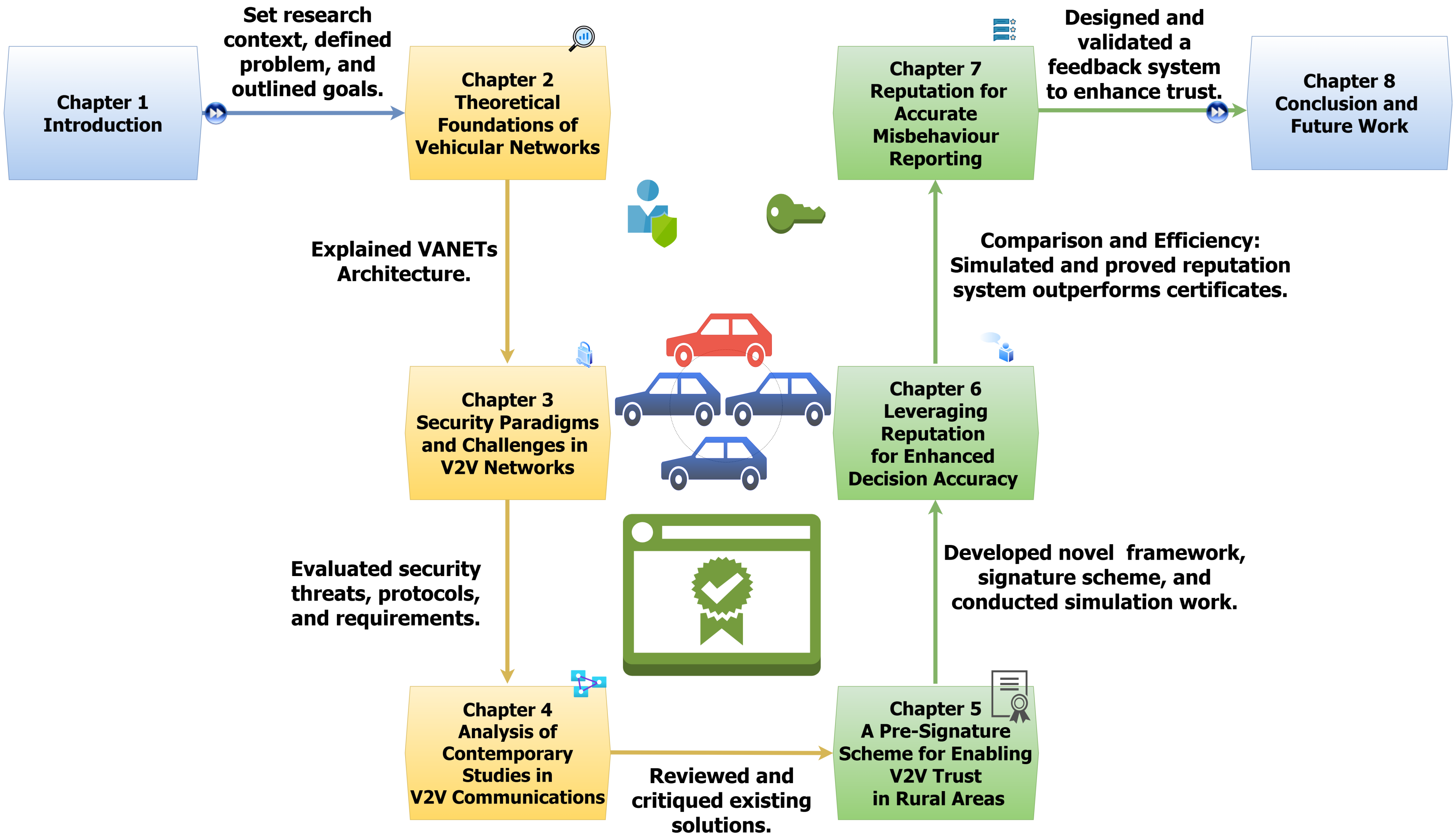

Chapter 1
Introduction
Set research context, defined problem, and outlined goals.
Chapter 2
Theoretical Foundations of Vehicular Networks
Explained VANETs Architecture.
Chapter 3
Security Paradigms and Challenges in V2V Networks
Evaluated security threats, protocols, and requirements.
Chapter 4
Analysis of Contemporary Studies in V2V Communications
Reviewed and critiqued existing solutions.
Chapter 5
A Pre-Signature Scheme for Enabling V2V Trust in Rural Areas
Developed novel framework, signature scheme, and conducted simulation work.
Chapter 6
Leveraging Reputation for Enhanced Decision Accuracy
Comparison and Efficiency: Simulated and proved reputation system outperforms certificates.
Chapter 7
Reputation for Accurate Misbehaviour Reporting
Designed and validated a feedback system to enhance trust.
Chapter 8
Conclusion and Future Work

Figure 1.3: Thesis Organisation.

Chapter 2

Theoretical Foundations of Vehicular Networks

This chapter introduces the main concepts to understand the discussions and research presented in this study. It provides an overview of Vehicular Ad-hoc Networks (VANETs) and discusses their structure and critical elements essential for vehicle communication. The chapter then explores the communication protocols used in VANETs, explaining their functions and technological foundations. Additionally, the discussion covers scenarios of disconnected environments in networks, outlining their characteristics with a detailed case study.

2.1 Introduction

Connected and Autonomous Vehicles (CAVs) are one of the most significant technological evolutions in Intelligent Transport Systems (ITS). They are a milestone in modern transportation and promise to revolutionize travel by enhancing safety, efficiency, and convenience. At the core of this transformation is the ability of these vehicles to communicate with each other and their surrounding infrastructure, a capability enabled mainly by VANETs. The more vehicles are connected, the more able they will be to obtain drastic enhancements in road safety and optimization of traffic flow and, consequently, to offer a full set of services for drivers and passengers. This chapter examines the key concepts of vehicular networks and their integration into autonomous vehicles, highlights the importance of network infrastructure and connectivity, and introduces a case study related to this research.

2.2 Core Concepts of VANETs

Vehicular Ad-hoc Network (VANET) is pivotal in the evolution of ITS, facilitating dynamic and self-organizing communication networks among vehicles. It is a type of mobile ad-hoc network (MANET) that is capable of the spontaneous creation of a network of mobile vehicles which is essential for enhancing road safety, optimizing traffic flow, and enabling various applications in smart transportation (Cunha et al., 2016). VANETs have been instrumental in the advancement of ITS, notably through two types of communications: Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V).

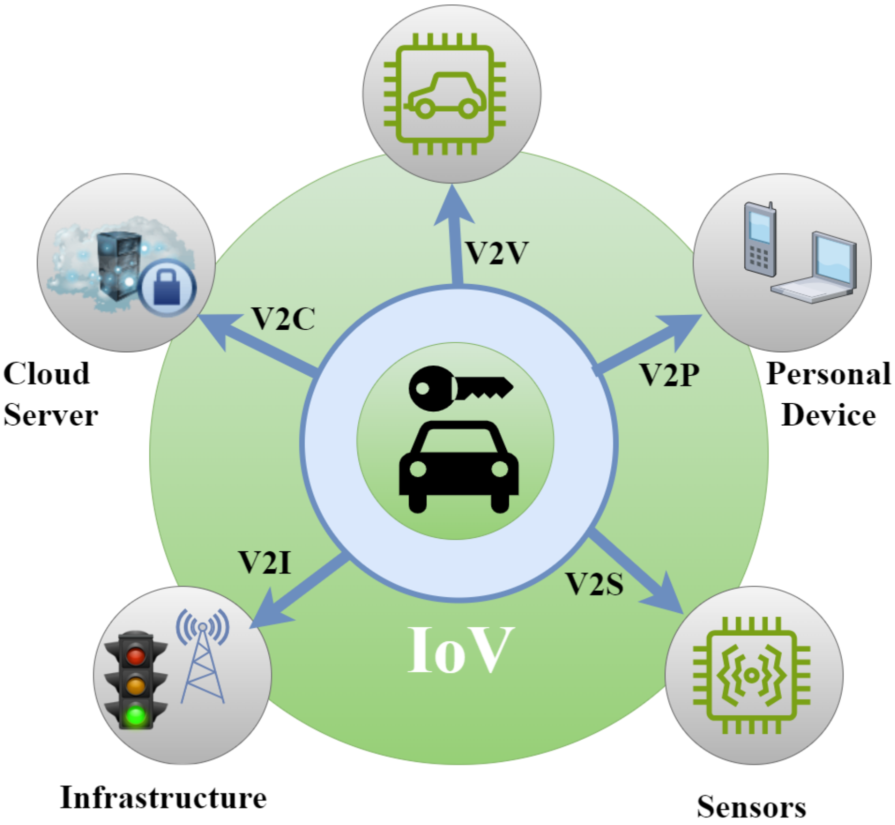


Figure 2.1: Types of Communications in IoV Network.

In V2V, the study's primary communication mode, vehicles move wireless access nodes, providing wireless connectivity to other vehicles and users in their surroundings. Expanding this concept is the Internet of Vehicles (IoV): A distributed network that maintains the use of Autonomous Vehicles (AVs) and the use of data created by vehicles. The concept of IoV, as shown in Figure 2.1, is built from intelligent vehicles that work collaboratively and interact with the surrounding environment using different types of real time communications (Duan et al., 2020). To illustrate, IoV technology is constructed based on the Vehicle to Everything (V2X) communication, where vehicles communicate with other surrounding elements such as: Vehicle to Sensor (V2S), Vehicle to Clouds (V2C), or Vehicle to Personal device (V2P). While IoV offers broader connectivity, VANETs are specifically related to V2I and V2V communications.

2.2.1 VANET Architecture

Vehicular ad hoc Network architecture is sophisticated and dynamic, designed to support frequent topology changes, high mobility, and real-time communication. As shown in Figure 2.2, VANETs facilitate direct communication between vehicles and between vehicles and the road infrastructure, creating reliable communications. The network infrastructure and the vehicles in VANETs are mainly considered intelligent nodes on the road, with their storage, sensors, and networking capabilities that distribute different messages.

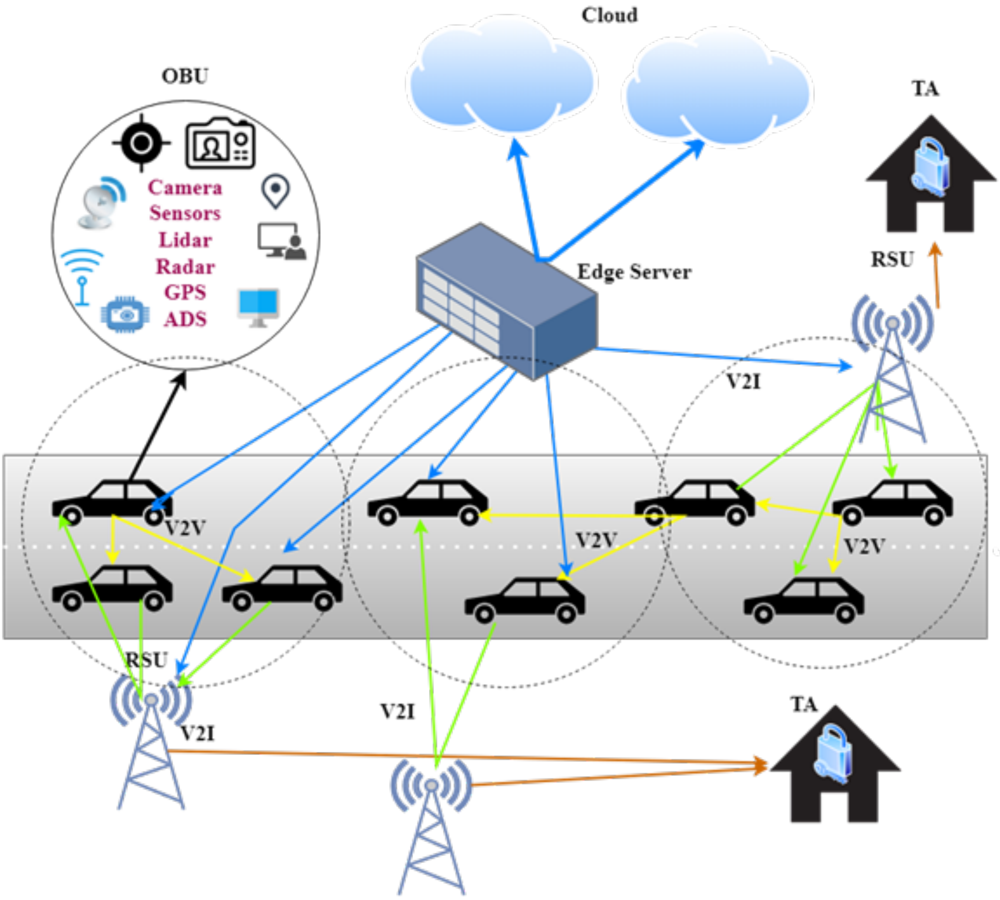


Figure 2.2: VANET Communications Architecture.

VANET has unique features that distinguish it from other wireless networks. These are a direct result of the specific requirements and challenges associated with vehicular communication (Amaouche et al., 2023), and are essential to understand vehicular communication systems and protocols.

- **Dynamic Topology:** VANET network topology is highly dynamic due to the high speed of the vehicle's movement. Vehicles (nodes) join and leave the network frequently, resulting in a constantly changing network structure. This necessitates the use of efficient routing algorithms that can quickly adapt to the changing topology.

- **High Mobility:** In VANETs, vehicles are constantly in motion, often at high speeds. This situation leads to rapid and frequent changes in the network topology, requiring efficient and adaptive communication protocols that can handle dynamic connections and disconnections.

- **Frequent Disconnections:** The dynamic nature and high mobility of VANETs result in disconnections between vehicles, which requires the development of some strategies to ensure reliable communication, such as the use of intermediate vehicles for data relay or store-and-forward techniques.

- **Low Latency Requirements:** Some applications in VANETs require real-time communication with very low latency. For example, in emergency situations such as collision avoidance scenarios, ensuring that messages are received promptly is critical for the effectiveness of these applications.

- **High Scalability:** VANETs need to be able to scale to accommodate a large number of vehicles, especially in urban settings with dense traffic. High scalability is crucial for maintaining communication performance as the number of connected vehicles increases.

- **Heterogeneity:** VANETs consist of diverse components, such as RSUs, traffic lights, sensors, servers, and vehicles like cars, trucks, and motorcycles. This heterogeneity requires the development of interoperable communication protocols that can seamlessly integrate diverse devices and technologies.

- **Non-Uniform Network Density:** VANETs' network density varies according to traffic density, which can be very high in a traffic jam or very low in suburban traffic. Nonuniformity should be considered when designing any vehicular network.

- **Energy and Processing Capacity:** The nodes in VANETs are vehicles that have sufficient energy, and enough space to include processing power and memory.

- **Geographical Communication:** Unlike other networks that use unicast or multicast to target specific nodes, VANETs introduce geographic communication, forwarding packets based on location (e.g., in safe-driving applications).

- **Security and Privacy:** Considering the sensitive nature of the shared data (e.g., driver information and vehicle positions), it is imperative to guarantee the security and privacy of communications in VANETs. This entails implementing robust security measures to guard against dangers, including data manipulation, spoofing, and attacks.

Analysing VANET architecture is essential to understanding the operation of such a complex network. This includes recognising the main protocols used to ensure reliable data transmission despite the rapidly changing network topology and the high-speed movement of vehicles. A deeper appreciation of VANETs requires exploring the specific components that constitute these networks. The next section delves into the primary components of a VANET, providing a detailed examination of their roles and functions that enable vehicles to communication and exchange data.

2.2.2 Main Components of VANETs

In a VANET, several components work together collaboratively to enable seamless data exchange and communication among vehicles (V2V) and between vehicles and infrastructure (V2I). This section identifies the primary components of VANETs, as shown in Figure 2.2: On-Board Units (OBUs), Roadside Units (RSUs), and the Trusted Authority (TA) (Hasrouny et al., 2017). Identifying these components is essential to understand how VANETs support a wide range of applications, from enhancing road safety to improving communication between autonomous driving technologies.

Table 2.1 summaries their functions and roles. Each vehicle is connected to the nearest RSU through its OBUs and the RSU can be connected to any number of vehicles under its coverage area. There is a set of RSUs under each TA , and under each RSU, a number of vehicles are moving on a road. TAs supply the OBUs and RSUs with a private key / public key and certificates. During the authentication process, TA provides the vehicle with certificates via the corresponding RSU. This process involves the use of encryption to secure the user's privacy (Li and Yin, 2022). More details on this process are discussed in later sections.

The following provides a more detailed explanation of the primary components, RSUs and OBUs.

Table 2.1: Outlining the Main Components of a VANET.

Unit	**Definition**	**Purpose**
OBU	A GPS-based tracking system embedded in each AV that allow the vehicles to communicate with each other and with RSU.	1-Retrieving the vital information. 2-Support vehicle electronics (e.g., resource command processor, sensors, user interfaces). 3-Communicate with RSUs and other OBUs via a wireless link.
RSU	A computing unit placed at fixed locations such as roads, intersections, and parking areas.	1- Provide (V2I) connectivity. 2-Support vehicle localization. 3-Connect vehicles with other RSUs using various network topologies. 4- Calculate vehicle trajectories to avoid threats.
TA	Oversees the entire VANET operation, ensuring only legitimate RSUs and OBUs can register and communicate.	1- Check OBU IDs. 2- Handle vehicle registration. 3- Maintain trust within the network. 4- Manage incentives, cryptographic keys, and certificates. 5- Detect malicious or suspicious behaviour.

1. Roadside Units (RSUs)

   In VANETs, the RSUs are located on the roadsides and connected to the Internet, allowing the OBUs of multiple vehicles to be connected. In this case, the RSUs act as hosts that provide services and the OBUs are peer devices that utilise the services provided by the RSUs. Moreover, the RSUs mainly register any vehicle that requests to participate in the network. First, the requested vehicle utilises the digital positioning system to detect and identify the nearby RSU. Then, the vehicle establishes communication with the connected RSU. The primary RSU functions are providing internet connectivity to the vehicle's OBUs, expanding the communication range between vehicles and providing safety applications such as collision avoidance (Amaouche et al., 2023).

2. On Board Units (OBUs)

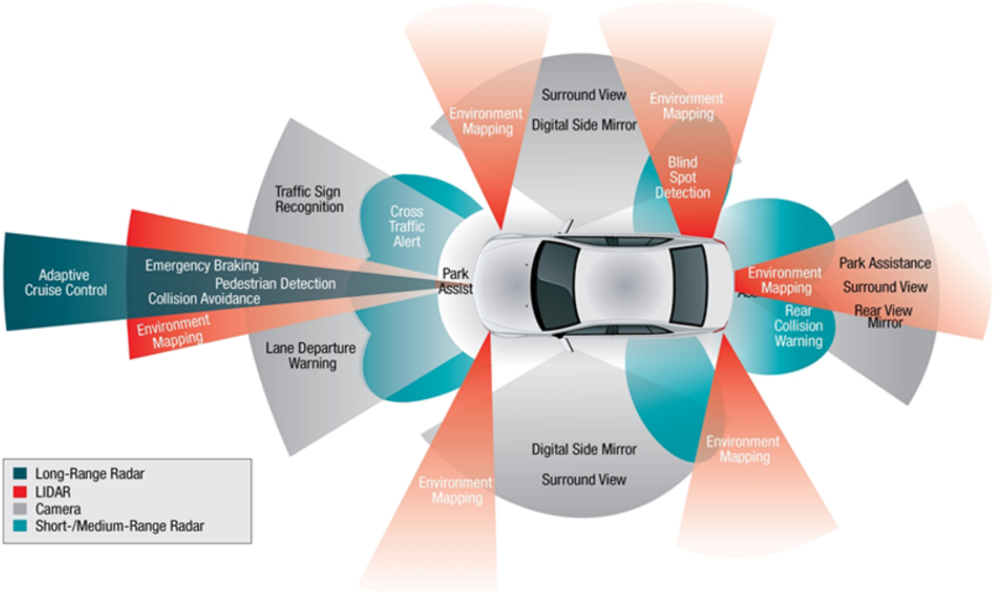


Figure 2.3: OBUs in Autonomous Vehicle.
Source: Machine Design

Each vehicle is considered an intelligent entity equipped with an efficient multi-sensor platform, computation units, communications tools, and IP-based connectivity in V2V either directly or indirectly, as shown in Figure 2.3. Additionally, a vehicle is envisioned as a multi-communication system that enables communications between intra-vehicle components, V2V, V2I, and V2X. OBUs provide the communications among vehicles V2V and between vehicles and RSUs.

During the communication, the OBUs detect any condition on the road and transmit status messages to other OBUs to support safety applications between vehicles (Pathrose, 2024). Table 2.2 outlines the purpose of each OBU.

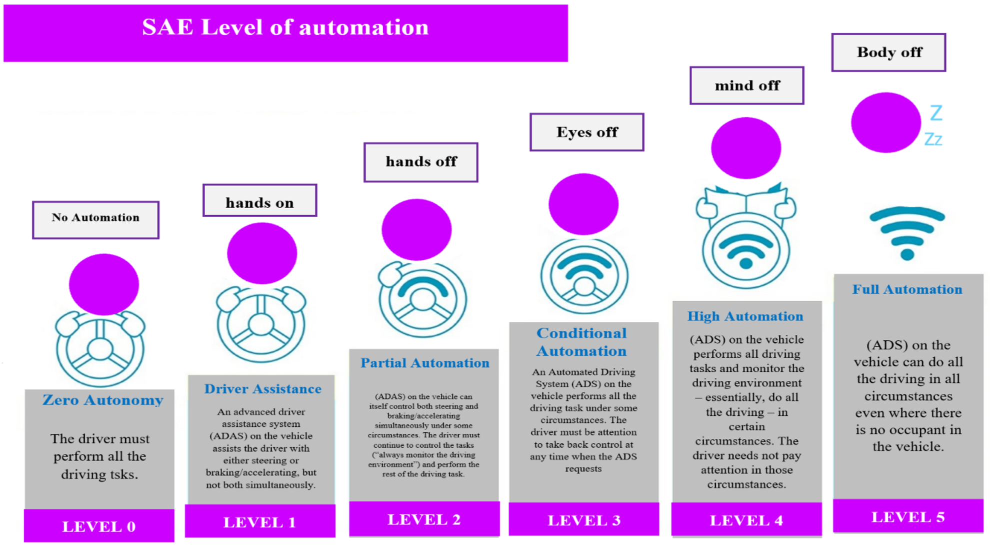
To summarize, RSUs and OBUs act as communication systems, allowing vehicles to communicate with each other and the surrounding environment instantly. This seamless interaction is essential for ensuring system safety, improving traffic flow, and facilitating intelligent transportation services.

Table 2.2: Outlining the Key Components of OBUs.

Unit	Purpose	Type
Central Processing Unit (CPU)	Handles general-purpose computing tasks.	Processing Unit
Graphics Processing Unit (GPU)	Manages intensive parallel processing tasks, essential for handling complex computations such as image and signal processing.	Processing Unit
Real-Time Operating System (RTOS)	Ensures timely processing of data and execution of safety-critical tasks.	Storage
Solid-State Drives (SSDs)	Fast and reliable storage solutions for large volumes of data generated by sensors and processing units.	Storage
Power Supply Management	Ensures consistent and reliable power supply to all the components of the OBU.	Storage
Inertial Measurement Unit (IMU)	Measures the vehicle's acceleration and angular rate.	Sensor
GPS	Provides precise location data.	Sensor
LiDAR	Provides high-resolution 3D maps of the surroundings.	Sensor
Radar	Useful for detecting objects at long ranges and in poor visibility conditions.	Sensor
Cameras	Capture visual information used for object detection, lane tracking, and more.	Sensor
Ultrasonic Sensors	Short-range sensors used for parking assistance and detecting obstacles close to the vehicle.	Sensor
V2X	Facilitates communication between the vehicle and external entities like other vehicles (V2V), infrastructure (V2I), and networks (V2N).	Communication Technology
Cellular Connectivity	Ensures constant communication with cloud services and other network-based resources.	Communication Technology

Understanding these components lays the groundwork for how they interact at various levels of automation, which will be the focus of the next section.

2.2.3 Levels of Automation in VANETs



The driver must perform all the driving tsks.

An advanced driver assistance system (ADAS) on the vehicle assists the driver with either steering or braking/accelerating, but not both simultaneously.

(ADAS) on the vehicle can itself control both steering and braking/accelerating simultaneously under some circumstances. The driver must continue to control the tasks ("always monitor the driving environment") and perform the rest of the driving task.

An Automated Driving System (ADS) on the vehicle performs all the driving task under some circumstances. The driver must be attention to take back control at any time when the ADS requests

(ADS) on the vehicle performs all driving tasks and monitor the driving environment – essentially, do all the driving – in certain circumstances. The driver needs not pay attention in those circumstances.

(ADS) on the the vehicle can do all the driving in all circumstances even where there is no occupant in the vehicle.

Figure 2.4: SAE Levels of Automation.
Source: (SAE International, 2021)

This section explores the automation levels highlighting the main advancements and technologies in each level and detailing how these technologies progress with time, enhancing vehicle control, safety, and efficiency. Outlining these levels is relevant for understanding the technological advancements in vehicular networks. The Society of Automation Engineers (SAE) identified six automation levels (SAE International, 2021), as shown in Figure 2.4 and described in Table 2.3. The levels of automation span from traditional manual driving systems (Level 0) to the fully autonomous driving (Level 5).

Vehicles become fully autonomous at higher levels of the taxonomy, and the passenger is not usually required to take action. To illustrate, the automation progresses from the basic level of connectivity to the full automation level. In (Level 0), the driver performs all the driving tasks and utilises basic applications like collision avoidance by sharing some information with other vehicles such as exchanging directions and speed.

Table 2.3: SAE Automation Levels.

SAE Level	**Description**	**Engagement level**	**User role**
0 Zero Autonomy	The driver must perform all the driving tasks	No Automation	Driver
1 Driver assistance	An advanced driver assistance system (ADAS) assists the driver with either steering or breaking/ accelerating, but not both simultaneously.	Hands on	Driver
2 Partial Automation	ADAS on the vehicle controls both steering and accelerating simultaneously under some circumstances. The driver must continue to control the tasks (monitor the driving environment) and performs the rest of driving task.	Hands off	Driver
3 Conditional Automation	An Automated Driving System (ADS) performs all the driving task under some circumstances. The driver must pay attention to take back control at any time when the ADS requests.	Eyes off	Passenger
4 High Automation	ADS on the vehicle performs all driving tasks and monitor the driving environment. Do all the driving- in certain circumstances. The driver needs not to pay attention in those circumstances.	Mind off	Passenger
5 Full Automation	ADS performs all the driving tasks under all circumstances, even when there is no occupant in the vehicle.	Body off	Passenger

Level 1 follows, with cooperative systems arising that support the vehicle's coordination of decisions, enabling some safety systems such as platooning and adaptive cruise control. As automation evolves, Level 2 (partial automation) uses an ADAS system to autonomously manage specific driving tasks by utilising real-time traffic information.

In Level 3 (conditional automation), the vehicle performs most of the tasks independently under specific conditions but still requires driver intervention when necessary. Level 4 follows with High automation in which the vehicle handles all driving tasks autonomously in several conditions. Finally, vehicles with full automation (Level 5) drive autonomously under all scenarios without any driver's intervention.

The established understanding of automated driving is constantly updated and now automatically recognizes the need for occasional driver control, even at high levels (Mutzenich et al., 2021). Drivers might need to reveal personal information to RSUs or other vehicles. Sharing some sensitive data such as user identity, IP address, video, and emotional state might put the vehicle or the driver in danger. In other words, large-scale data collection makes exploiting personal information more accessible and lucrative; hence, the attacker will find it an attractive environment in which to launch attacks, as explained in the following chapter. Providing secure communication to ensure the vehicle's safety is the main goal in implementing VANET safety applications where vehicles can send and receive emergency messages to each other to ensure user safety (Bintoro, 2021).

Consideration needs to be given to the implications of the different automation levels in the event of an attack. This issue is highlighted because the user in L0-L2 is often expected to be aware of the situation and be fully responsible, whereas, in L3-L5, as the focus levels of this study, the situation will be different. A vehicle or user may have to respond to confusing traffic situations, such as accidents and congestion, understanding the automation levels and the user's role in each level is critical in such challenging situations. For example, in sudden emergency scenarios in L3-L5, drivers are expected to maintain adequate situational awareness.

Yet, they may be engaged in other activities such as using social media or sleeping, which can impair their responsiveness. As automation evolves from low to high levels, Internet connectivity is anticipated to rise accordingly. Despite this, the study is conducted in disconnected environments where exchanging messages is the sole communication way. Therefore, users at L3-L5, which are the primary focused levels in this study, need to understand the communication protocols for exchanging messages in order to react appropriately and make the right decisions to these messages in such a challenging environment as explained in the following section.

2.3 Message Exchange in Vehicular Networks

VANETs ensure prompt broadcasting of safety messages between vehicles and RSUs, enabling timely alerts during traffic congestion and accidents (Mariani, 2018). This section presents an overview of V2V communication protocols, followed by an explanation of the main communication protocol involved, Dedicated Short-Range Communication (DSRC). Additionally, this section explores the different types of messages in V2V networks, providing a detailed description of each.

2.3.1 Communication Protocols in V2V

Various communication protocols are designed to ensure reliable, timely, and secure transmission messages exchange. Each protocol is tailored to address specific requirements and challenges and they are vary based on routing positions, communication strategies, and other factors (Abbasi and Shahid Khan, 2018; Yogarayan et al., 2020). Table 2.4 outlines the main protocols in V2V communications based on their attributes.

Table 2.4: Main Communication Protocols in V2V.

Protocol	**Type**	**Frequency Band**	**Range**	**Speed /Rate**	**Main Features**	**Applications**
DSRC	Wireless Short-Range	5.9 GHz	Up to 1 km	Up to 27 Mbps	Low-latency, high-speed, robust to mobility, safety-critical messages	Basic safety messages (BSMs), accident avoidance
C-V2X	Cellular-based V2V	LTE, 5G	Wide coverage	High data rates	Device-to-device and network-based modes, higher reliability, broad coverage	Basic safety, advanced driver assistance systems (ADAS)
AODV	Reactive Routing	Dynamic	Varies	Dynamic	On-demand routing, reduces overhead, adapts to dynamic topology	Dynamic routing, emergency message dissemination
Geocast Protocols	Geographic Routing	Dynamic	Geographic area	Dynamic	Disseminates messages to specific geographic areas, ensures relevant delivery	Incident alerts, localised traffic information
Broadcast Protocols	Broadcast	Dynamic	Varies	Dynamic	Broadcasts messages to all vehicles within range, ensures widespread dissemination	Safety messages, congestion alerts
VIEP	Information Exchange	Dynamic	Varies	Dynamic	Reliable, timely data transmission, prioritizes safety-critical messages	Safety and non-safety message exchange

Requirements-based differences between technologies can be observed in Table 2.4, where each technology offers features specific to the goal of communication. Advanced qualifications are offered, such as those supporting the cellular networks-based Cellular Vehicle-to-Everything (C-V2X) technology. Dynamic and efficient route establishment by Ad hoc OnDemand Distance Vector (AODV) and the Dedicated Short-Range Communication (DSRC), which are considered the most effective routing protocols in VANETs that maintain continuous connectivity between vehicles (Khan et al., 2022).

Message dissemination protocols, such as geocast broadcasting, are vital in efficiently communicating safety-critical messages across communication ranges and maintaining high-level intervehicle/ surroundings interaction. However, it is worth noting that the main protocol for providing real-time communications in VANETs is DSRC, which supplies a foundation for direct (V2V) or (V2I) connectivity using Wireless Access in Vehicular Environments (WAVE) that is based on the IEEE 802.11p standard defines the radio physical and Medium Access Control (MAC) layer link. Since this study is being conducted in a rural area, DSRC is the primary protocol used to support V2V communications. The following section provides a detailed exploration of DSRC, examining its functions, features, and importance in enabling vehicle communication, even in challenging scenarios.

2.3.2 Dedicated Short-Range Communication

Dedicated Short-Range Communication (DSRC) serves as a wireless protocol specifically designed to facilitate high-speed communication over short distances, both among vehicles and between vehicles and infrastructure.

The Global System for Mobile communications (GSM) and other traditional cellular technologies lack the distinctive advantages of DSRC, particularly its high-bandwidth and low-latency capabilities, which are vital in difficult weather circumstances or high-speed situations (Kenney, 2011).

DSRC is the international Wireless Access in Vehicular Environments (WAVE) initiative standard. The primary objective of DSRC is to enable the instantaneous exchange of critical information, with a particular focus on applications like collision avoidance and traffic management. Operating within a range of 300 to 900 m, DSRC allows vehicles to effectively communicate with each other as well as with the RSUs when they are nearby (Kenney, 2011). However, a notable challenge arises in disconnected environments where the absence of nearby RSUs complicates or renders impossible the standard verification process for received messages. Despite this challenge, DSRC remains pivotal in advancing safety and efficiency in V2V communications which makes it the primary protocol used in this study.

As shown in Figure 2.5, the 75MHz spectrum is classified into eight channels: one reserved channel with 5MHz and seven channels with 10MHz including five service channels (172,174,176,180,182) and one control channel (178).

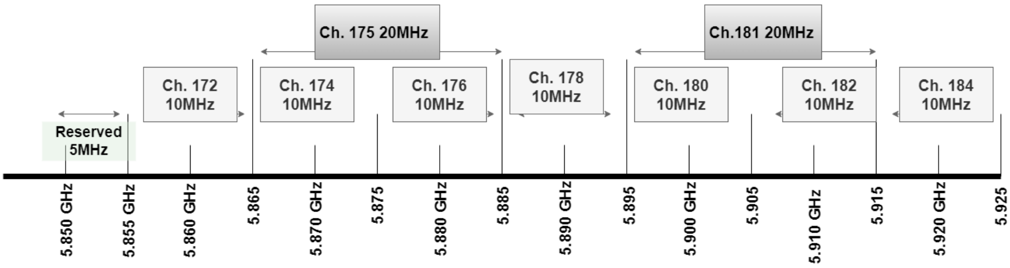


Figure 2.5: Frequency and Channel Division of DSRC.

According to the American Intelligent Transportation Association, 172 is the channel used for V2V communication, and channel 184 is used for safety and non-safety DSRC operations. Additionally, channel 178 is a control channel for establishing a communication link among OBUs or between RSUs and OBUs (National Research Council US, 2000). In this system, if either the vehicle's OBU or a RSU intends to send a message and then detects that another message is currently being processed on the channel, it must wait until the ongoing process is ended before sending its message. The control channel controls the process based on set priorities, where non-secure communication is given low priority, and safety communication is given high priority.

DSRC's protocol stack, as shown in Figure 2.6 is designed to handle the rapid changes and high mobility in the system topology characteristics of vehicular networks. DSRC supports the WAVE Short Message Protocol

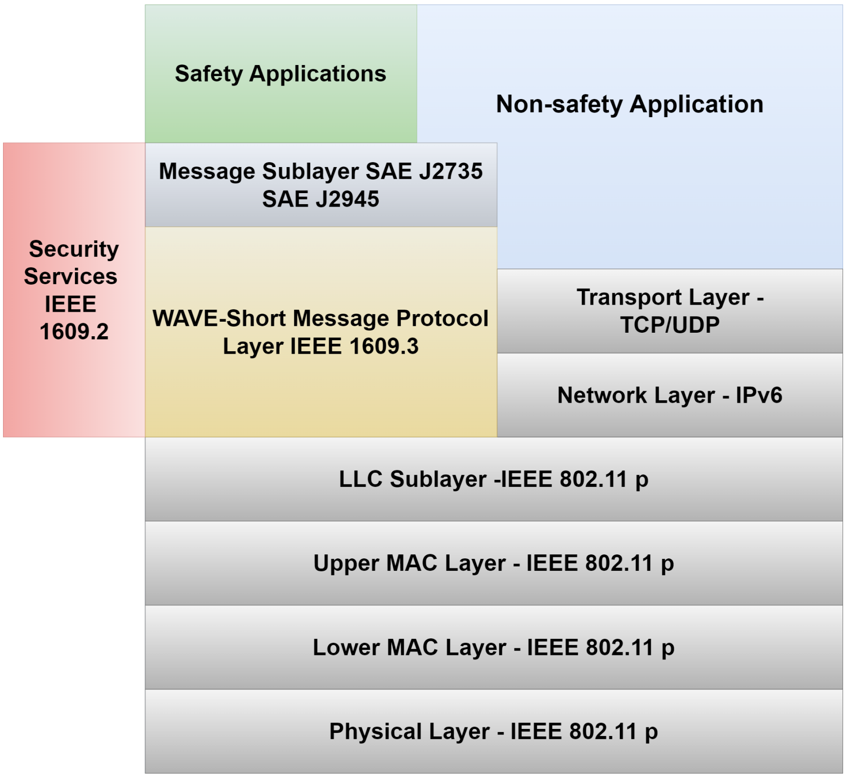

Safety Applications
Non-safety Application
Message Sublayer SAE J2735 SAE J2945
Security Services IEEE 1609.2
WAVE-Short Message Protocol Layer IEEE 1609.3
Transport Layer - TCP/UDP
Network Layer - IPv6
LLC Sublayer -IEEE 802.11 p
Upper MAC Layer - IEEE 802.11 p
Lower MAC Layer - IEEE 802.11 p
Physical Layer - IEEE 802.11 p

Figure 2.6: DSRC Protocol Stack.

(WSMP) and transport protocols IPv6. WSMP is created to exchange non-routing data, such as security information as defined in IEEE 1609.2. The physical layer of the DSRC stack is based on the IEEE 802.11p standard, a revision of IEEE 802.11a, using a 10 MHz bandwidth. The Logical Link Control (LLC) layer uses IEEE 802.2 protocol, utilising 0x86DC for WAVE Short Message (WSM) and 0x86DD for IPv6. While these short messages can be disseminated in any channel in a single-hop manner, IP packets can be transmitted over the service channel for transport routing packets in a multi-hop network. DSRC upper layer standards consist of the Society of Automotive Engineers (SAE) J2735 (Dedicated Short Range Communications Message Set Dictionary) and J2945 (Dedicated Short Range Communication Minimum Performance Requirements) (SAE International, 2020).

SAE J2735 specifies a set of DSRC-based message standards, including message content and frame format, whereas SAE J2945 defines the minimum performance requirements and Basic Safety Messages (BSM) for V2V communications (Khan et al., 2022). Further details about these messages and their types are explained in the next section.

2.3.3 Safety Messages in V2V Communications

VANETs encompass a variety of Basic Safety Messages (BSM), each with a specific purpose of ensuring vehicle safety and efficiency. One of the main concerns in designing VANETs is the reliable dissemination of these messages to all the related vehicles in the communication. The primary aim is to limit the message transmission latency of such information as well as to ensure the receiver makes the right decision regarding these messages as soon as an emergency occurs. BSM can be categorised into six types according to purpose and priority (Wu et al., 2024).

Table 2.5: Types of Safety Messages in VANETs.

Message Type	**Description**	**Comm. type**	**Priority**
Group Communication	Vehicles that share the same features can participate in this communication. E.g., vehicles that have the same models or vehicles sharing the exact location in the time interval.	V2V	Low
Road Condition Warning	Nearby Vehicles exchange safety messages about the condition of the road (e.g., congestion, maintenance, closed road, etc.)	V2V	Medium
Low Connection Warning	The exchange messages contain information about the VANET connection conditions in some areas (e. g. type of wireless and the communication speed. etc.)	I2V V2V	Medium
Collision Warning	In different collision situations, safety messages are needed to be sent to a nearby vehicles to avoid further incidents and increase safety. (e.g., post and pre-crash warning.)	V2V	High
VANET Warning	Warning messages alert nearby vehicles to incidents affecting the VANET, such as disruptions or attacks.	V2V V2I	High
I2V Warning	The infrastructure broadcast messages via RSUs to all vehicles within its surrounding area about environmental weather and safety issues when an issue is detected.	I2V	High

As outlined in Table 2.5, Priority reflects the urgency of each message type and transmission speed. A high-priority message, such as a collision warning message, limits accidents, while a low-priority message, such as group communication, can be less time-sensitive. In this way, alerts will be delivered promptly.

This research specifically focuses on the primary type of collision warning messages known as Decentralised Environmental Notification Message

(DENM). These messages play a vital role in alerting vehicles by delivering timely and critical information in emergency V2V scenarios, thereby helping to limit accidents and enhance overall road safety (Marzouk et al., 2018). DENM is one of the safety messages that utilises the DSRC broadcasting technology to alert vehicles about the status of the road. By doing this, the nearby vehicles gather data on the relevant event, which they can utilise for autonomous cooperative driving or the ADAS. During communications, when a vehicle detects an incident, it alerts other vehicles by generating and broadcasting DENM messages. These messages might reach up to one kilometres, though practical implementations follow the National Highway Traffic Safety Administration's (NHTSA) recommendation of an effective range of 300 metres (Kahn, 2015).

DENM messages contain critical information that inform vehicles about road conditions and any obstacles or emergencies. The structure of DENM is illustrated in two parts in Figure 2.7. Part I includes a message count, temporary ID, and main vehicle data such as time, position, speed, heading, and acceleration. These frequent updates are sent more frequently, approximately 10 times a second, to enable real-time awareness and immediate threat detection. In Part II, additional critical information describing a specific event is distributed regularly, but less frequently and only when necessary.

In compliance with IEEE 1609 standards for Wireless Access in Vehicular Environments (WAVE), DENM messages are orchestrated via IPv6 multicast channels over 802.11p/ETSI G5. On the vehicle side, the Vehicle ITS Station Mobile Router both generates and forwards externally received DENMs into the in-vehicle network. Meanwhile, WAVE Short Message (WSM) utilises IEEE 802.11p for wireless communication and IEEE 802.11e for quality of service at the MAC layer (Xie et al., 2023).

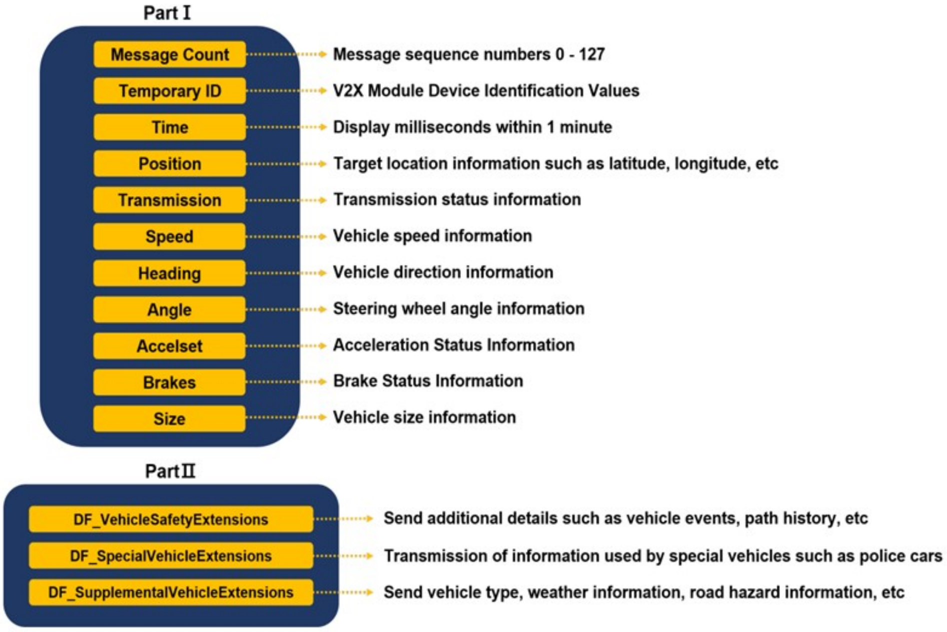

Part I
Message Count
Temporary ID
Time
Position
Transmission
Speed
Heading
Angle
Accelset
Brakes
Size
Message sequence numbers 0 - 127
V2X Module Device Identification Values
Display milliseconds within 1 minute
Target location information such as latitude, longitude, etc
Transmission status information
Vehicle speed information
Vehicle direction information
Steering wheel angle information
Acceleration Status Information
Brake Status Information
Vehicle size information
PartII
DF_VehicleSafetyExtensions
DF_SpecialVehicleExtensions
DF_SupplementalVehicleExtensions
Send additional details such as vehicle events, path history, etc
Transmission of information used by special vehicles such as police cars
Send vehicle type, weather information, road hazard information, etc

Figure 2.7: Structure of the DENM Message Part I; Part II.
Source: (SAE International, 2020)

Continuing this stack, DENM messages follow the WAVE Short Message Protocol (WSMP) and are defined based on SAE J2735. VANET entities generally manage message handling via a First-In-First-Out (FIFO) buffer. WSMP safety messages operate above the IEEE 1609.3 layer by passing the TCP/IP protocol stack entirely, as stated by Papadimitratos (2024). Figure 2.8 illustrates the format of WSM used in this research.

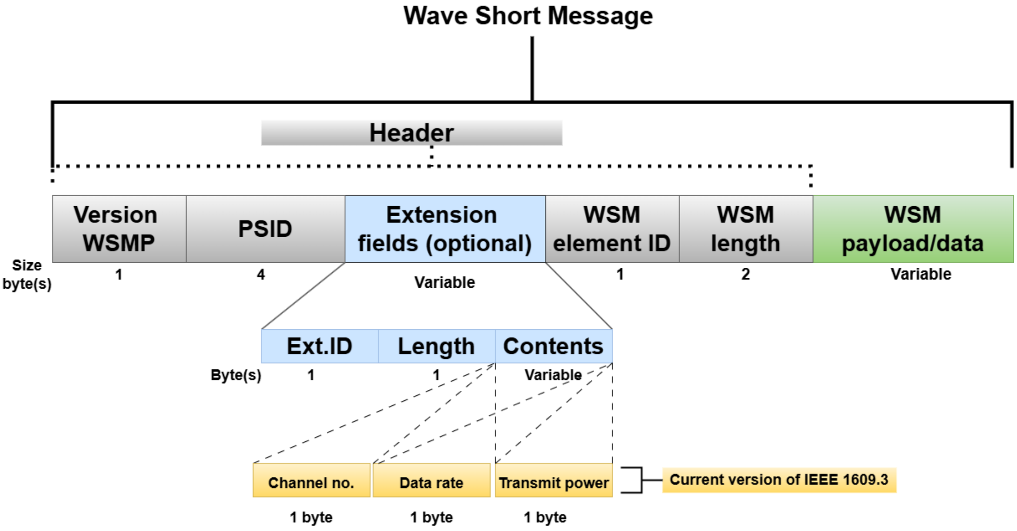


Figure 2.8: Message-Format-of-WAVE-Short-Message-WSM.

At the top (the header), the message includes fields for the WSMP version, a Provider Service Identifier (PSID), and any optional extension fields. These optional extensions appear as an Ext. ID, a Length, and various Contents allow message customisation (e.g., specifying channel number, data rate, or transmit power).

Following the optional fields, the header specifies the WSM element ID (identifying the data type carried) and the WSM length(defining how many bytes the payload occupies). After the header, the WSM payload/data region contains the information transmitted, such as safety alerts or traffic updates used by vehicles and RSUs in a VANET.

Having explored the V2V transmission technologies and protocols, it is relevant to consider how they are used in practice. While this is arguably straightforward in scenarios with suable supporting infrastructure, it is also relevant to consider how vehicles communicate within more challenging environments. As such, the following section discusses the nature of disconnected zones and a case study example that is used within this research.

2.4 Disconnected Areas of Vehicular Networks

Despite the advancements in V2V communications, some locations still have connectivity issues. For example, in rural areas with limited connectivity or in disaster-hit regions where infrastructure is damaged, the traditional methods of online verification are not feasible. Moreover, potentially harmful to the safety and efficiency of vehicular networks as a whole. This section describes these disconnected areas addressing their features, effects, and possible measures. It also gives an overview of the selected area in this research, including its geographical location, main features, and importance within the research context.

2.4.1 Characteristics of Disconnected Areas

As V2V communications enable direct interaction between nearby vehicles in disconnected areas, Internet connectivity is limited or unavailable, which affects critical communication among vehicles. This factor makes the task of maintaining continuous connectivity between vehicles in such conditions a very difficult challenge. This is commonly the case in non-residential and outside the urban locations: tunnels, mountains, or remote locations where RSUs are not deployed. While GSM communications technologies are certainly widespread, they are not universally accessible, due to geographic limitations. For example, from GSMA website (GSMA, 2025), it is clear that the coverage in the some areas is not always guaranteed, and it is easy to find many places in different countries where there is road infrastructure but a lack of 2G coverage (let alone coverage from 3G or higher networks). Although satellite communications can offer greater coverage, they do so with limited capacity, higher latency, and at a cost that may not be considered viable.

As stated by the World Bank (2024), the world's rural population is approximately 43% of the overall global population. A study by Davis et al. (2023) showed that within the United States, about 46 million people reside in rural areas, constituting about 13.8% of the total U.S. population compared to 20% in Canada, 56% in the European Union (EU), and 60% in China. These low signal areas have structural or geographical attributes that affect the wireless signals to propagate properly and thus cause weak or no connectivity between vehicles and infrastructures (Agrawal et al., 2016). The lack of connectivity in these areas is not just a function of physical obstructions but are tied to ecosystem triggers and infrastructural determinants as well (Mistareehi, 2021).

To explain, geographical characteristics such as valleys, dense forests, and cliffs are expected in disconnected locations, and they are all to be placed in separate random/exact spots on the map. By blocking the line-of-sight required for robust wireless communication, these obstacles cause signal attenuation and failure. Additionally, these regions might experience extreme weather conditions, including heavy rain, fog, and snow, which can further degrade signal quality. The combination of physical obstructions and adverse weather conditions creates an environment where maintaining continuous communication is inherently difficult.

Infrastructural challenges are a major factor contributing to the lack of connectivity in these regions. The deployment of communication infrastructure(e.g., cell towers, RSUs) is often impractical due to the high costs associated with installation. Maintenance and operational issues compound the problem, particularly in extreme environments where equipment can fail long before repairs are possible (Makkawi et al., 2015). As a result, many of these areas either have insufficient RSUs or remain entirely outside the communication network's coverage. The lack of connection extends beyond the technology portion, as it has real-world ramifications for vehicle safety and operational efficiency. The real-time data transmission and reception of safety messages have been greatly affected because they can not make vehicles communicate to RSUs or trusted authorities on a regular basis. The following section delves deeper into the description of the selected area in this study, providing a description of this area and the main reasons for choosing it as a case study.

2.4.2 Case Study of Disconnected Areas

In order to provide a real-world context for understanding the problem and basing the later simulation work, this research focused on vehicular communication in the Peak District. This is a National Park in central England, and the map view in Figure 2.9 illustrates the sparse environment compared to nearby population centres.

Peak District environment is characterised by high levels of disconnected areas and low infrastructure density, both critical difficulties that the research can investigate solutions to address. As shown in Figure 2.10, Peak District is known for its rocky terrain and many hills, valleys, and extensive cave systems that make it difficult to provide continuous connectivity. Nonetheless, as also shown in each of theses pictures, there are roads throughout the area, and consequently the potential for vehicles and related incidents. In this sense it is typical of many other rural regions.

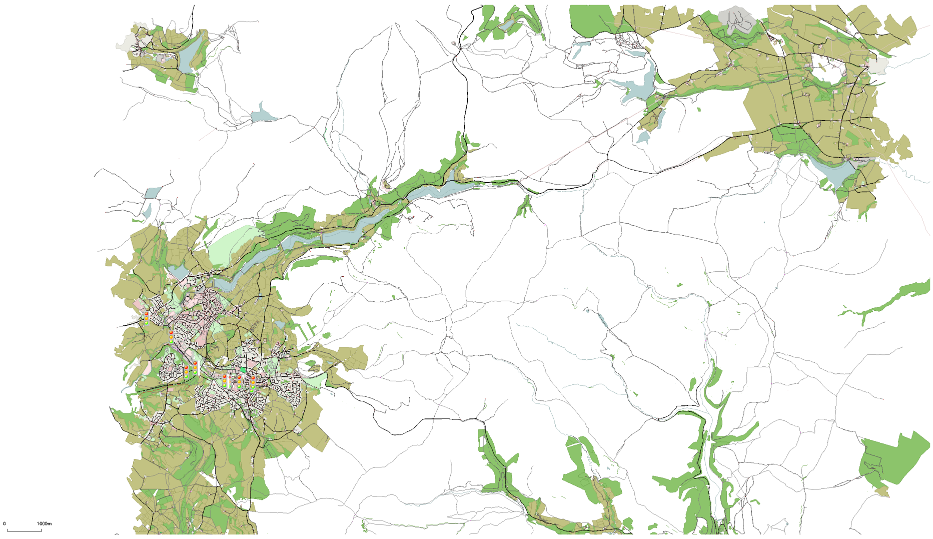


Figure 2.9: Peak District Map Extracted from OpenStreetMap (OSM).

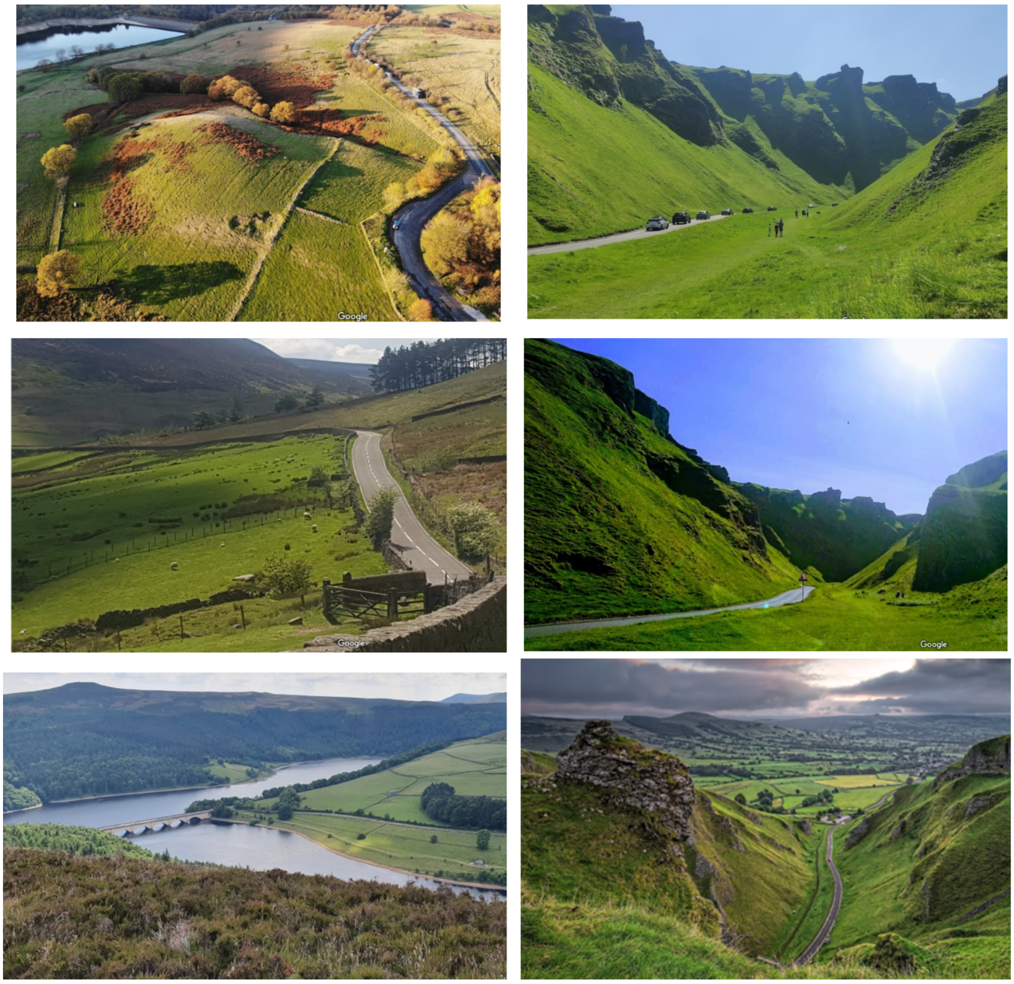


Figure 2.10: Peak District Environment Extracted from Google Map.
Source: (Google Maps, 2025)

The natural and geographic features of the Peak District make it challenging to deploy RSUs and maintain infrastructure in the traditional communication network. RSUs play an essential role in authenticating communications and making them more reliable, which enhances VANET security levels at large (Yu et al., 2022). However, deploying the RSUs is a complex process in the environment like peak district.

The absence or inadequate deployment of RSUs in these disconnected regions poses a significant hazard to the efficiency and reliability of VANETs. As a result, it compromises the overall serviceability of many vehicles operating in these challenging scenarios. For example, the absence of RSUs in this area causes frequent signal loss and weak communication reliability.

Therefore, the lack of infrastructure in the Peak district underscores the urgent need to manage connectivity issues in an area where RSU deployment is insufficient or low.

While vehicles in such situations rely on DSRC as the primary communication protocol, vehicles need to rely on a reliable and secure system to evaluate the exchanged messages, especially in emergencies (Abualola et al., 2022). The following section explores and validates various mitigation strategies in a real-world setting to overcome obstacles in these types of environments.

2.4.3 Mitigation Strategies for Disconnected Areas

To counter the effects of disconnectivity in rural areas, a verity of mitigation strategies have been proposed and implemented. Table 2.6 summarizes various mitigating strategies related to expected communication issues in VANETs. Each of these countermeasures addresses different issues when being configured in low connectivity areas. The table indicates the individual vulnerabilities of each approach, thereby creating a more rounded understanding of their potential limitations and implementation considerations. Each technology serves a specific purpose and boosts connectivity in different ways. However, none of them provides a real-time connectivity or full communication between vehicles (Daddanala et al., 2021; Tahir et al., 2022). To illustrate, in challenging scenarios like rural areas, vehicles need a reliable way to communicate and make the right decisions during emergencies. DSRC utilises a dedicated spectrum for vehicle communication and stands out as the only communication protocol that vehicles can rely on for such critical situations (Clancy et al., 2024).

Table 2.6: Connectivity Mitigation Strategies for Disconnected Areas.

Strategy	**Description**	**Weakness**
Fiber-Optic Cables	Wired communication backbone (high-capacity, low-latency).	High installation costs, difficult deployment and rugged/ inaccessible terrains.
Signal Boosters and Repeaters	Signal boosters/range extenders where devices amplify and retransmit the signal.	Extra latency and need frequent maintenance in harsh environmental conditions.
Mobile RSUs	Flexible units installed on Vehicles to establish a temporary mobile communication.	Operational in constrained timeliness and range, may need to be manually deployed.
Adaptive Signal Processing	This class of techniques includes everything from noise filtering to interference cancellation and mitigation.	Complex algorithms and computational overhead. Increases the implementation complexity and the costs.
Weather-Resilient units	Communication devices built to last through all weather conditions.	Higher prices, and higher rates for expert installation and maintenance.
Delay-Tolerant Networks (DTNs)	Networks offer temporary communication over scarce infrastructure.	Not suitable for real-time applications, possible delay of data transmission.

2.5 Conclusion

The chapter described the basic principles on which autonomous vehicle information communication is based and how vehicular networks have become indispensable in supporting these services. This ground knowledge is thus used in analysing and developing further advanced solutions in order to enhance the reliability and security features of VANETs, especially under challenging conditions. Moving on to the next chapter, it becomes obvious that vehicular networks have a number of advantages. However, such networks' open and highly dynamic nature makes communications susceptible to attacks/threats that deteriorate safety and dependability, possibly compromising safety and reliability systems.

Chapter 3

Security Paradigms and Challenges in V2V Networks

This chapter discusses common security issues within vehicular networks, including potential attack scenarios. The discussion then provides an overview of the main security requirements needed to mitigate different challenges and situations in vehicular communications, highlighting the central standard Vehicular Public Key Infrastructure (V-PKI), Security Credential Management System (SCMS) that utilised certificates to facilitate data transmission between vehicles for more secure and authenticated communications.

3.1 Introduction

The overview of Autonomous Vehicles (AVs) and vehicular communication in the previous chapter sets the stage for understanding the security vulnerabilities that these systems may encounter. As AVs optimise V2V communications in the Intelligent Transport Systems (ITS), ensuring the security of VANETs becomes ever more essential. By addressing these challenges, this chapter aims to provide a comprehensive foundation for enhancing the security of vehicle communication systems. This discussion delves into the critical security systems and issues that underpin these technologies. As explained, vehicular networks are critical in allowing vehicles to communicate with each other and the infrastructure for real-time data exchange that improves the safety, efficiency, and functionality of communications. However, the openness and dynamic nature of VANET makes it vulnerable to various threat scenarios bringing various security problems that must be solved to guarantee an efficient and safe network. The chapter provides an overview of the SCMS processes and certificate management, focusing on the PCs and the CRL.

3.2 Security Threats and Attacks

As previously explained, a particular concern in VANETs is the ability to disseminate alerts and emergency messages effectively and securely via the V2V/V2I nodes, given the diminishing involvement of vehicle users in some critical scenarios during communications. With this challenge in mind, this section analyses the security attacks in vehicular networks. It considers a range of related attack scenarios that could be encountered, each of which illustrates contexts in which users may need to be made aware and make accurate decisions in response.

3.2.1 Security Attacks Analysis

Different attack activities, such as jamming, spoofing, and interference, can affect vehicular communications, reducing stability, robustness, real-time security, and privacy. These situations will make the network unable to provide effective services and even cause severe problems affecting vehicles and networks. In VANETs, the classification of attacks can be approached from various perspectives. For example, attacks can be classified on their level of potential impact, which would include the type of impact and the risk of it occurring, such as high versus low risk. Attacks also can be classified based on their nature, such as active versus passive attacks (Zhu et al., 2014), active attack either sends a fake message or fails to forward the correct received messages, while a passive attack remains covert, only monitoring communication without interference such as a selfish behaviour. In addition, attackers can be classified based on their origin, such as insider versus outsider attacks (Pooja et al., 2014), the insider attack is an authenticated vehicle with deep knowledge of the network configuration, while the outside attack is authenticated vehicle, with limited capability to attack the network compared to insider attackers. Some studies classified the attacks according to the layer of the application they target, including application layer attacks and network layer attacks or they classified them based on their targets (Goyal et al., 2022).

Table 3.1 outlines the most common attacks chosen for their relevance and impact on security based on different factors such as the targeted security requirement, the communication types, the damage level, and the mitigation strategy. After outlining the attacks, it is essential to demonstrate their impact on the security requirements critical to vehicular network integrity, confidentiality, and availability. These requirements are explained in detail in (*Section* 3.3.1).

Table 3.1: Comparison of Security Attacks in VANETs .

Attack Name	**Threatened Security Requirement**	**Comm Type**	**Damage Level**	**Possible Defense Mechanisms**
Sybil	- Authentication - Identity Management	V2V/V2I	High	- Group or radio signatures - PKI - Reputation systems
DOS	Availability	V2V/V2I	High	- PKI and authentication - Rate limiting - Intrusion detection
Timing	- Integrity - Authentication	V2V/V2I	High	- Robust time-stamping - Anomaly detection - Secure sync protocols
Replay	-Integrity - Authentication	V2V/V2I	High	Timestamps / nonces - Sequence numbers - Anti-replay protocols
Black hole	Availability	V2V	Moderate High	- Watchdog monitoring - Trust-based routing - Intrusion detection
Gray hole	Availability	V2V	Moderate High	- Selective packet drop detection - Reputation/trust systems - Routing oversight
Wormhole	- Availability - Integrity	V2V	Moderate High	- Time/distance bounding - Wormhole detection protocols - Location verification
Malware	- Integrity - Availability (Confidentiality)	V2V/ V2I	Moderate High	- Secure boot - Anti-malware software - IDS / firewall
Illusion	-Integrity - Authentication	V2V /V2I	Moderate High	- Sensor/data fusion - Consistency checks - Intrusion detection

Figure 3.1 shows the attack activities on the security requirements. This illustration allows for an understanding of how different attacks in VANETs can target specific aspects of network security.

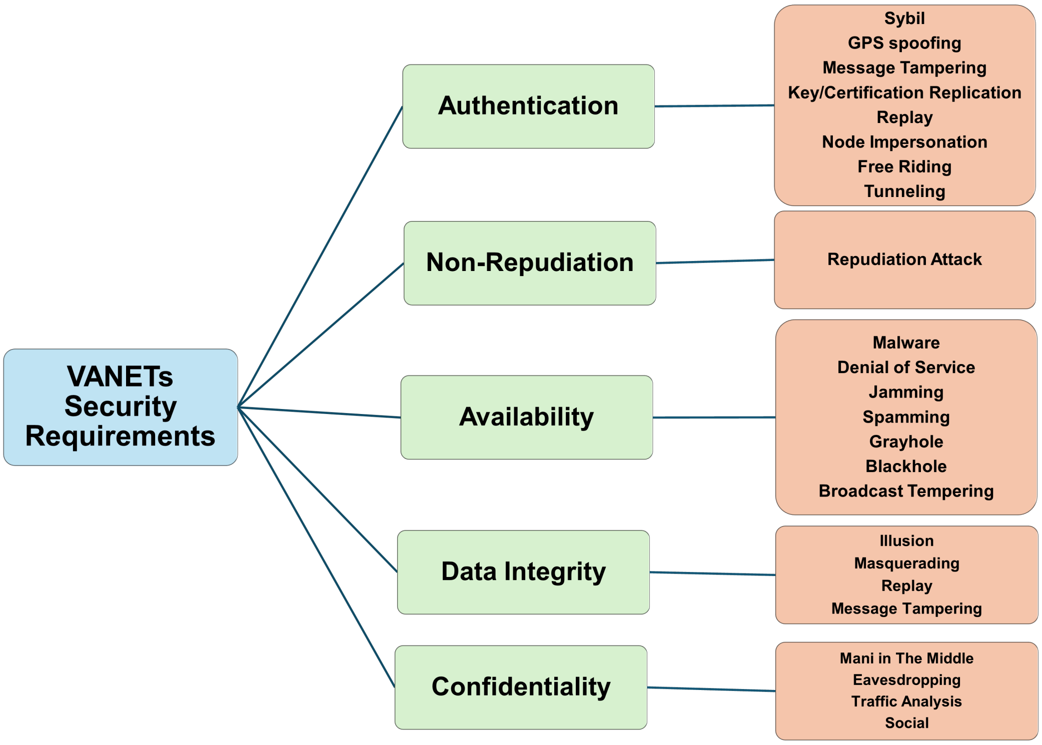


Figure 3.1: Taxonomy of Security Attacks Targeting Services in VANETs.

These attacks can be grouped into five main categories: attacks on authentication, availability attacks, routing attacks, data authenticity attacks, and secrecy attacks (AlMarshoud et al., 2024).

- **Attacks on Authentication:** Authentication attacks are highly risky, such as when convey vehicles are compromised regarding their identities or honesty. These attacks can have serious consequences, including unauthorised access and control over critical vehicular data, causing severe service disruptions and safety hazards. This type of attack can be classified into four common attacks as follows:

  1. Sybil Attack: Sybil's attack in vehicular networks was initially explored by Douceur (2002). It is considered one of the most serious threats to V2V communication. It occurs when a malicious vehicle generates multiple false and illegal identities. This type of attack causes havoc by controlling most nodes, eventually disrupting traffic. As the primary focus of the research,

this attack is critically investigated in later chapters due to its potential to severely compromise the trust and reliability of the V2V network.

2. GPS Deception Attacks: GPS deception provides a vehicle with fake information about its location, speed, and other GPS functions. Once the vehicle accepts this information, safety or financial issues will occur, which cause fake evidence and unpredictable property damage (Wen et al., 2005).
3. Wormhole Attack: It means that two or more malicious nodes conceal the true distances between them to lure more normal nodes to route in a risky path. In this case, nodes absorb data from the routing nodes, which makes the network cooperate with other attackers (Ali et al., 2022). In such a case, each element loses its typical response when attacked by wormholes, which affects the routing algorithm.
4. Masquerading Attack: In VANETs, each node is assigned a unique identification, a crucial aspect of the network's functionality. However, the disruptive potential of masquerading attacks, which can allow multiple nodes to share the same ID, cannot be overstated (Chaouche et al., 2023). Such an event could throw the network into disarray, rendering it unable to function correctly.

- **Attacks on Availability:** Availability Attacks mean that the Attacker can affect the availability of the vehicular networks; the Attacker uses bandwidth and transmission capacity limitations to bring the network down. In such a type of attack, Channel Interference and Denial of Service attacks are the most common types of attacks on availability (Houmer and Hasnaoui, 2020; Gaba et al., 2023).

1. Channel Interference Attacks: Channel interference attacks interrupt the communication in VANETs by interfering with the wireless / radio communication channels. This type of attack is also referred as a Jamming attack.

2. Denial of Service (DoS) Attacks: In VANETs, different types of communication take place between V2V and V2I that are exposed to DoS attacks. In a DoS attack, the attacker disrupts vehicular communication by flooding the network with fake requests, which overwhelms the network and makes it ignore legitimate requests from the user (Raghuwanshi and Jain, 2015).

3. Distributed Denial of Service Attacks: DDoS attack is an advanced form of DoS attack where an attack can be launched on several systems towards a particular system and then disrupt the target system functionality (Vamshi Krishna and Ganesh Reddy, 2023).

- **Attacks on Confidentiality:** Confidentiality in VANETs is vulnerable to attacks which target interception and access of sensitive information transmitted among vehicles including location data, driving patterns or personal details about drivers. Indeed, these kinds of attacks contribute to privacy violations in which unauthorised parties discreetly obtain private data and potentially exploit it in malicious ways (e.g., stalking or blackmail). Additionally, lack of confidentiality can damage the trust in the network which may lead drivers to abstain from V2V communication offerings. It is also important in VANETs that the confidentiality of all data transmitted must be preserved (Hamdi et al., 2021). There are four primary attacks under this type, as listed below.

1. Man-in-the-Middle Attack: This attack is the part of V2V communication wherein an attacker may intercept the message and modify it between two vehicles. Victims can believe in private one-on-one communication even with oversight communication.

2. Eavesdropping: Wireless communications are broadcast in nature and thus routing nodes are always susceptible to eavesdropping. This kind of attack is hard to detect because it does not alter or disrupt the original data being transmitted.

3. Traffic Analysis Attack: This attack poses a serious threat to confidentiality by enabling information disclosure. An attacker monitors message transmission frequencies, identifying periods of high information content after intercepting and analysing the transmitted messages.

4. Social Attack: An attack that sends inappropriate or unethical messages to drivers in order to distract them and see if they respond.

- **Data Integrity Attacks:** V2V communications may also be affected by attacks targeting data integrity, as these can compromise the trustworthiness of information exchanged among vehicles and thus result in imprecision or perhaps deception. These actions compromise the accuracy of transmitted data and erode trust between vehicles. Data integrity attacks can be classified into four main types (Hamdi et al., 2021):

  1. Illusion Attack: This attack manipulates some sensors to generate false information inside the VANET communications.

  2. Replay Attack: In this type of attack, a large number of messages are replayed, increasing the cost of precious bandwidth,

and then the priority messages are dropped from the queue. Because of the frequent replaying and deleting, the efficiency of the VANETs' system would be significantly declined (Al-shareeda et al., 2020).

3. Camouflage Attack: This attack occurs when a malicious node disguises itself with a false identity to spread deceptive messages, enabling black-hole or other critical attacks in the network.

4. Message Fabrication and Tampering with Messages: An attacker carries out fabrication attacks, creating bogus routing messages that are challenging to detect since they are received as valid routing packets from malicious vehicles.

- **Attack on Non-Repudiation:** An attack on non-repudiation in VANETs means that a sender denies having sent a message, or the recipient denies having received it, affecting the network's trustworthiness. One way that non-repudiation could be attacked is by an adversary who forges or mutates messages to make the actual sender unknowable, thereby undermining the reliability of communication. These attacks have serious consequences, such as the false accusation of other innocent vehicles or the concealing of malicious vehicle identity that disrupts vehicular communications integrity. One of the examples of this attack is the Repudiation Attack.

3.2.2 Potential Attacks Scenarios

In this section, a focus on the attacker scenarios and behaviours in launching attacks on VANET will be stated. For example, users need to broadly announce specific messages in real-time (e.g., emergency messages) but selecting a trusted node to store and disseminate critical information poses a challenge. Figure 3.2 depicts a range of scenarios that some attacks launched in VANET, specifically at L3-L4 automation. These scenarios provide a better understanding of the practical implications, potential attacks and security threats against vehicular networks.

- **Scenario A:** The scenario depicts a Sybil attack (Figure 3.2 A), in which the attacker (red vehicle) has different fake identities to disrupt the standard operation. First, the attacker broadcasts multiple counterfeit messages. Then, it manipulates other vehicles' directions. For example, the attacker may broadcast congestion ahead; if the victim vehicle acts upon this, it is forced to alter its paths and exit. In this case, AV users should react quickly to confirm the safety messages received by RSU to thwart such attacks.

- **Scenario B:** In broadcast tampering, the attacker creates false safety messages to hide traffic threats, which can lead to situations like accidents and road congestion. As shown in (Figure 3.2 B), the attacker broadcasts fake messages, "there is no congestion ahead, and the road is clear," to mislead other vehicles to continue straight. The white front vehicle, for example, will continue proceeding and then encounter congestion. Users can identify the attack by monitoring the AV sensors, ignoring the fake message, and exiting the road.

  Moreover, users can safeguard the VANET by alerting other vehicles on the road and broadcasting a corrective message.

- **Scenario C:** This attack occurs during V2V communications (Figure 3.2 C). The attacker checks the target vehicles closely and then alters the messages between them. In this case, the attacker manipulates the V2V communications while the victims think they communicate privately.

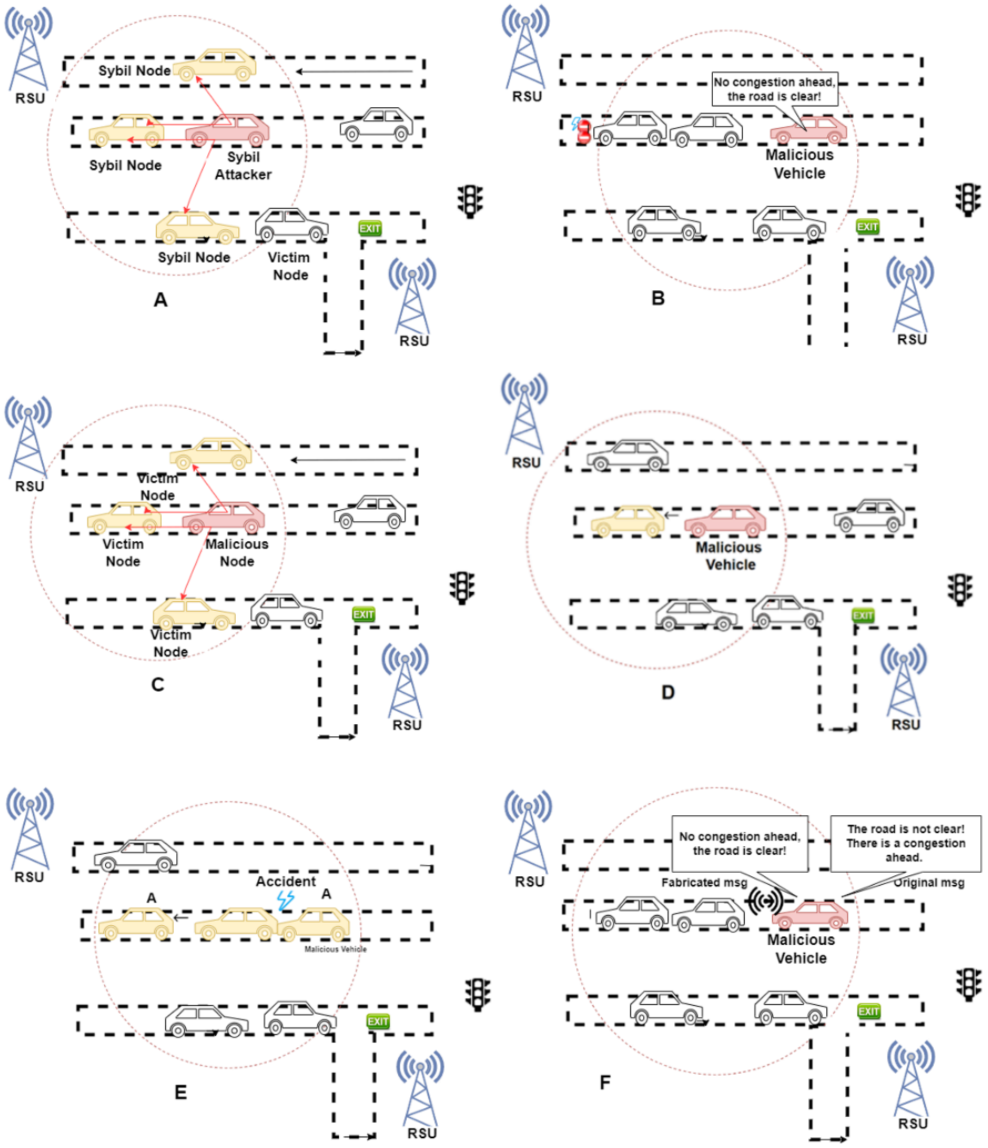


Figure 3.2: Scenarios of Vulnerability to Malicious Attacks in VANETs.

- **Scenario D:** A masquerading attack occurs when the attacker logins into the VANET system using a stolen ID and passwords then attempts to broadcast false messages which appear to come from the registered vehicle (Bagga et al., 2020). For example, in (Figure 3.2 D), the red vehicle pretends to be police, then forces the yellow front vehicle to expose information such as an ID or a social number. In this case, AV users need to be aware of this situation and know how to react to deny revealing information to the untrusted vehicle; they also need to check the accuracy of received messages with the Trusted Authority before starting the communication.

- **Scenario E:** In this scenario, two or more vehicles share the same key. The two vehicles will not be distinguished, so their actions can be repudiated. With this stolen identity, as shown in (Figure 3.2 E), the malicious vehicle (A) spreads fake messages over the VANET to mislead other vehicles regarding road conditions or hazards. An attacker may deny the accident and the related message since all the vehicles would appear identical to the shared key. This strategy, known as repudiation, enables the malicious vehicle to avoid accountability, compromising integrity and trust in the VANET system.

- **Scenario F:** This depicts a replay attack, in which the malicious vehicle replays the previous message's transmission to exploit its contents at the moment of transmission. As shown in (Figure 3.2 F), a malicious vehicle alters a duplicate of the received message then resends it again to the neighbouring vehicles causing further VANET incidents.

While the notion of VANETs is fundamentally aimed towards reducing or removing the need for human involvement, it is still crucial to define what responsibilities users may still be required to fulfil (such as roles and duties, control transfer, operational mode, and most importantly, decision making). Security, legal and ethical responsibilities need that occupant to remain aware of the VANET situation. After outlining the attacks compromising this technology, it is crucial to address how to interact with security standards to report threats, emphasizing secure credential usage and vigilance to strengthen network security. The following section investigates more security requirements in vehicular communications, paving the way for a detailed discussion on the SCMS on which vehicles rely to authenticate during communications.

3.3 Security Requirements and Challenges

Building on the discussion of attacks in the previous section, this section first outlines the key requirements needed to address these threats. Then, it explores the challenges associated with effectively implementing these requirements.

3.3.1 Security Requirements

Security is one of the essential concerns to guarantee the privacy, safety, and reliability of that network during communications among vehicles, as well as between infrastructure and any vehicle. As stated earlier, due to the high mobility and decentralised architecture of vehicular networks, these types of wireless communication can be affected by many security threats, such as illegal access issues, denial of service or even data modification attacks. Hence, stringent security mechanisms are inevitable to maintain trust among users, increase the security of processing and data exchange, preserve the privacy of sensitive information, and ensure the overall resilience and functionality of the network in real-world scenarios. The security requirements include the following:

1. **Authentication** (Identity Protection). Vehicles need to be able to authenticate themselves and the infrastructure to protect VANETs from internal and external attacks so that malicious vehicles will not submit false messages into the network. As explained in the following section, digital certificates are widely used to verify VANETs, typically managed by PKI and SCMS.

2. **Availability** (Continuous Service). The operations in VANETs have to be operative and reachable for time-critical services, particularly traffic safety applications.

3. **Confidentiality** (Establishment of Privacy and Security). Some communications among VANETs may exchange personal information, such as vehicle identifiers, location, or both. Preventing these data from being eavesdropped through encryption is necessary for privacy concerns.

4. **Non-Repudiation** (Accountability in Communication). It ensures that once a vehicle has delivered its messages, no one can claim it did not send them. This is important in resolving conflicts, especially in accident reports, where the source of a message can always be debated.

5. **Privacy** (Ensuring Anonymity). With vehicles sending and receiving different messages, drivers' anonymity needs protection. Methods like pseudonymity allow messages to be authenticated while preserving a vehicle's or driver's true identity.

6. **Scalability** (Scaling and Security). VANETs need to scale up in size without losing their security properties. These security mechanisms must handle certificates and keys on a scale over such an extensive network fast and without delays.

7. **Low Latency** (Real-Time Communication). The security mechanisms in VANETs have to be performed in real-time or with as little delay as possible. Due to the high mobility of the vehicle, any safety-critical messages on its network must meet the timely delivery property.

8. **Revocation** (Trust Management). Trust-management infrastructure is necessary to promptly revoke certificates from vehicles that have been compromised or are behaving suspiciously. Efficient and scalable revocation facilities should be provided to make revoked entities no longer valid in the network.

9. **Data Integrity** (Data Protection). This ensures that the message received is exactly what was sent, digital signatures are used for message and data integrity to preserve the integrity of critical exchanged information such as safety alerts and traffic updates.

10. **Data Validation** (Verification). Verification ensures that messages exchanged between vehicles are accurate and originate from trusted sources. Checking data consistency with related messages is crucial to prevent misleading information and ensure data accuracy, particularly between nearby vehicles, which is essential for secure communication, maintaining network integrity, and reliability.

11. **Robustness Against Attacks** (Resilience to Malicious Activities). VANETs are going through different attacks, such as the Sybil attack in which a vehicle claims multiple wrong identities and disseminates

incorrect information during communication, specifically in emergencies to mislead vehicles. Hence, security protocols must be robust to resist these and other potential threats.

3.3.2 Security Challenges

Ensuring security during vehicle communications is the primary process in implementing VANETs. This process prevents attackers from inserting fake information or altering the correct messages. During communication, especially in emergencies, driver accountability is vital to providing accurate real-time messages about traffic conditions. However, VANETs' dynamic and decentralised nature raises critical security challenges, making correct real-time messages exchange challenging in some scenarios. Addressing these challenges is essential to provide safe and reliable communication between vehicles. It is worth noting that unique security challenges may occur due to VANET's distinct characteristics. The following points illustrate some security challenges in VANETs:

1. **Lack of Standards:** Heterogeneity in communication protocols in VANETs makes effective V2V communication and connection difficult and prohibits ease of scaling. VANETs involve various communication standards and protocols (e.g., DSRC, cellular networks) that need to interoperate seamlessly, which can be complex to manage. A proper communication standard system can be achieved by adapting open standards and current, closed, and one-way systems, which will be integrated into an effective system for seamless communication and smooth information exchange.

2. **Dynamic Topology:** VANETs are self organised networks which allows vehicles to join and leave the network autonomously as they travel. Due to vehicle movement and varying traffic densities, the network structure in a VANET changes frequently, affecting connectivity and routing stability.

3. **Delay Constraints:** In applications like collision avoidance and emergency notifications, time is crucial for ensuring that all packets are delivered safely and in real time. This requires specific strict delay constraints, with either no or very low service delay.

4. **Precise Vehicle Positioning:** Accurate positioning is required for safety applications, as inaccuracies can compromise reliability and system performance. The industry standard for vehicle positioning, the Assisted Global Positioning System (AGPS), is not fully protected (Pandey et al., 2023). It provides the vehicle location up to five to ten metres precisely, which is not sufficient for a secure and reliable network that requires long-term planning.

5. **Sustainable Service:** As VANETs are a new, upcoming technology, providing an intelligent and user-friendly system is challenging. The network must maintain scalable and well-organised communication among vehicles.

6. **Fault Tolerance:** Exchanging information over VANETs requires highly reliable network communications that can provide real-time communication even in the presence of malicious nodes (Karabulut et al., 2023).

7. **Infrastructure Dependency:** Many VANET services rely on roadside infrastructure, which may not be available in rural or underserved areas, leading to connectivity issues.

8. **Poor Network Connectivity:** Network connectivity is the main factor in VANET. However, poor and unstable internet connectivity in some rural areas and environmental factors such as buildings, weather, and traffic can interfere with signal quality, reducing communication reliability.

9. **Security and Privacy:** Security and privacy are the foundations of any network. Identification of vehicles is essential to make ad hoc decisions and secure user data. Otherwise, anyone can trace the vehicle, which will be a security hazard for the vehicle and passengers. For example, data may be misused to locate passengers' travelling interests and visited places, which causes serious issues (Shahabi and Soni, 2023). Hence, security and privacy are two significant challenges that must be addressed. This concern is the primary focus of this research, and it has been reviewed in detail in the following sections.

Having outlined the security requirements and challenges, it is essential to consider systems capable of addressing the security and privacy issues effectively. The Security Credential Management System (SCMS) emerges as a well-established framework designed explicitly for vehicular networks, offering security and privacy solutions to critical challenges such as authentication and message integrity, as explained in the following section.

3.4 SCMS Role in Vehicular Networks

Vehicular Public Key Infrastructure (V-PKI) networks have been deployed globally to enable secure vehicle communication. The main initiatives are European Telecommunications Standards Institute (ETSI) and Car-to-Car Communication Consortium (C2C-CC) in Europe (European Telecommunication Standard Institute ETSI40, 2021), SCMS in the US (Brecht et al., 2018), Secure Communication Module for Electric vehicles (SCME) in China (Tao et al., 2019), and others are dedicated to establishing robust communication frameworks and efficient credential management systems for both vehicles and infrastructure, significantly enhancing the effectiveness and security of transportation systems.

While these systems serve similar functions in providing secure and privacy-preserving vehicular communication, SCMS stands out to be a standardised solution to secure the communications in VANETs. This thesis focuses on the SCMS while incorporating elements of the ETSI for broader alignment. SCMS has several key advantages compared to its alternatives: broad applicability, robust misbehaviour reporting, hierarchical trust management, and strong privacy from certificates (Chen et al., 2024).

The system ensures trust among vehicles by exchanging anonymised data and utilising Pseudonym Certificates (PCs) with short durations. Within the SCMS framework, the Pseudonym Certificate Authority (PCA) collaborates with the Misbehaviour Authority (MA), Linkage Authorities (LA1 and LA2), and Registration Authority (RA) to identify the linkage values for adding vehicle information to the Certification Revocation List (CRL) in case misbehaviour is detected (Khan et al., 2020). Explaining each authority process is essential to understand the architecture of SCMS.

The following subsections describe these authorities in detail, highlighting the two main processes in this system: the generation of the certificates and the revocation of certificates. Leading to a discussion of the main challenges related to these process in V2V communications.

3.4.1 SCMS Architecture Overview

Since autonomous and connected vehicle technology exchanges critical information between vehicles and between vehicles and roadway infrastructure such as RSUs, traffic management centres, and wireless mobile units, a security management system is needed to ensure vehicle safety, security, and privacy. The U.S. Department of Transportation (U.S. DOT) formed the Crash Avoidance Metrics Partnership (CAMP) with the automobile industry and security specialists to create and develop a proof-of-concept (POC) security solution that gives users confidence in the system and each other (U.S. Department of Transportation, National Highway Traffic Safety Administration, 2018). A standard security solution called Security Credential Management System (SCMS) is used for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication.

To enable trusted communication, SCMS uses a Public Key Infrastructure (PKI) based strategy that leverages advanced techniques for certificate management and encryption. Authorised system participants use digital certificates provided by the SCMS to authenticate and verify crucial safety and mobility messages for connected vehicle technologies. These certificates protect the privacy of vehicle owners and operators by excluding any personal or equipment-identifying details, serving instead as system credentials to establish trust in the origin of each message. The SCMS's primary role includes securing message content by isolating and eliminating misbehaving vehicles and preserving user privacy (Brecht et al., 2018).

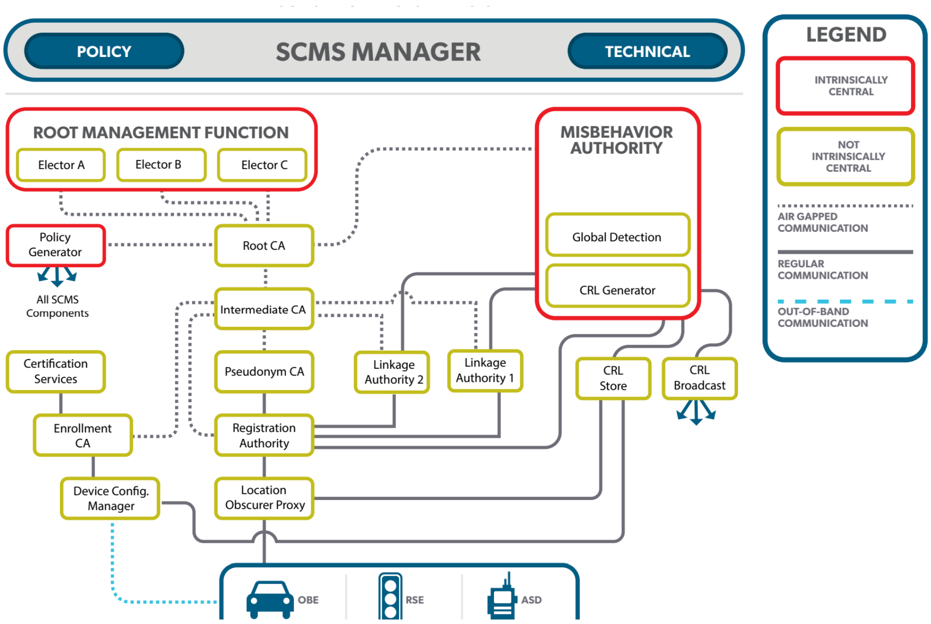


Figure 3.3: SCMS Architecture Design.
Source: (Brecht et al., 2018)

Figure 3.3 outlines the SCMS architecture: The SCMS Manager, Misbehaviour Authority (MA), the Root Management Functions (electors A,B,C) and Policy Generator (PG) are centrally located authorities within the SCMS. The lines linking various authorities in the system which represent relationships where one authority transmits information or certificates to another in at least one use case. Initially designed for V2V applications, the SCMS was expanded to support V2I scenarios (Whyte et al., 2013).

Figure 3.3 presents infrastructure-originating broadcast messages (e.g. traffic light announcements) and service announcements and provisioning (e.g., Internet access). Broadcast messages require authentication by roadside equipment (RSE), while service provisioning necessitates that onboard equipment (OBE) in the vehicle establish a communication channel with the RSE. Even if a vehicle is solely engaged in V2V operations, it can still report misbehaviour and receive revocation information regarding vehicles participating in V2I activities (such as infrastructure components), and vice versa. The SCMS comprises four types of connection:

- Solid Lines: Represent regular, secure communications, including certificate bundles.

- Dashed Lines: Depict the credential chain of trust, showcasing the trust chain for signature verification. Enrolment certificates are validated using the ECA certificate, while pseudonym, application, and identification certificates are verified against the PCA certificate. Certificate revocation lists are authenticated using the CRL Generator certificate (a component of the MA). This line does not suggest data transfer between the connected components.

- Dash-Dotted lines: Denote Out-of-Band communications, for example, the line connecting the RSE and the Device Configuration Manage.

- Connections designated with Location Obscurer Proxy (LOP): This proxy anonymizes requests by removing all location-related information.

All interconnecting online elements use a secure and reliable communication channel, utilising protocols like those in the Transport Layer Security (TLS) suite (Rescorla, 2018). Specific components like the Root CA and the Electors are physically isolated from the system. Data is encrypted and verified at the application layer when passing through an SCMS component that does not have direct access to the data. For instance, data produced by the Linkage Authority for the PCA may pass through the Registration Authority without being accessed directly by it. As stated by Whyte et al. (2013); Brecht et al. (2018), the SCMS design encompasses the following components:

- SCMS Manager: The manager is responsible for ensuring efficient and equitable operation, defining organizational and technical policies, and establishing guidelines for reviewing misbehaviour and revocation requests to ensure procedural correctness and fairness.

- Certification Services: Define the certification process and outline the types of vehicles eligible to receive digital certificates.

- CRL Store: A straightforward pass-through authority that stores Certificate Revocation Lists (CRLs).

- CRL Broadcast: The authority that disseminates the current CRL through channels such as RSEs or satellite radio systems.

- Device: An end-entity (EE) device responsible for sending or receiving messages, such as an Onboard Equipment (OBE), an RSE, or a Traffic Management Center (TMC) backend.

- Device Configuration Manager (DCM): It validates the Enrolment Credential Authority (ECA), ensuring a vehicle can receive enrolment certificates. It also supplies all necessary configuration settings and certificates during the bootstrapping process.

- Electors: Electors are the cornerstone of trust within the SCMS and are responsible for signing ballots that approve or reject an RCA or another elector. The SCMS Manager then distributes these ballots to all SCMS authorities, including devices, to establish trust relationships between RCAs and electors. Each elector possesses a self-signed certificate, and all entities in the system inherently trust the initial set of electors. Consequently, all entities must protect electors against unauthorised modifications once the initial set is installed.

- Enrolment Certificate Authority (ECA): This component issues enrolment certificates that serve as a vehicle's passport for authentication against the RA when requesting certificates. Various ECAs may issue enrolment certificates tailored to specific geographic regions, manufacturers, or device types.

- Intermediate Certificate Authority (ICA): This component acts as a secondary CA, protecting the root CA from traffic and malicious attacks. The Root CA issues the certificate for the ICA.

- Linkage Authority (LA): This authority generates pre-linkage values crucial for forming linkage values embedded in certificates to support efficient revocation. The SCMS features two LAs, LA1 and LA2, to prevent the operator of an LA from linking certificates associated with a specific vehicle.

- Location Obscurer Proxy (LOP): This proxy conceals the location of the requesting vehicle by altering source addresses, thus preventing the mapping of network addresses to physical locations.

- Misbehaviour Authority (MA): It manages misbehaviour reports to detect potential misconduct or device malfunctions. If necessary, the MA revokes and blacklists such vehicles on the CRL after linking their certificate identifier to the corresponding enrolment certificates. This authority comprises two sub-authorities: Global Misbehaviour Detection, tasked with identifying misbehaving vehicles, and CRL Generator (CRLG), responsible for creating, digitally signing, and releasing the CRL to the public.

- Policy Generator (PG): This component manages and creates updates for the Global Policy File (GPF) and the Global Certificate Chain File (GCCF), which store global configuration information and trust chains for the SCMS.

- Pseudonym Certificate Authority (PCA): This authority issues short-term pseudonyms, identification, and vehicle application certificates. Individual PCAs may be restricted by geographic region, manufacturer, or vehicle type.

- Registration Authority (RA): This authority validates and processes vehicle requests, generating specific certificate requests for the PCA. The RA enforces measures to prevent revoked vehicles from receiving new certificates and to ensure that vehicles receive only one set of certificates within a specific time frame. It also shares verified SCMS configuration updates with vehicles, including changes in network addresses or certificates and policy decisions from the SCMS Manager.

- Root Certificate Authority (RCA): RCA is the foundational element at the top of the certificate chain within the SCMS, acting as a trusted anchor in a conventional PKI context. It is responsible for issuing certificates for Intermediate Certificate Authorities (ICAs) and key SCMS components such as Policy Generator (PG) and MA.

Notably, the SCMS architecture guarantees that no single entity possesses or creates a full dataset that would allow vehicle tracking. While the RA holds the enrolment certificate for a vehicle requesting PCs, it cannot access the content of the certificates delivered by the PCA, as they are encrypted during transmission. Each PC is generated separately by the PCA without knowing the recipient or which certificates the RA assigns to a particular vehicle.

3.4.2 SCMS: Pseudonym Certificates

To ensure message integrity, authentication, and vehicle privacy, Pseudonym Certificates (PCs), are typically issued by the PCA in the SCMS. PCs are used for short periods to safeguard privacy and are periodically changed, to prevent message linkability. This section focuses mainly on the PCs process for vehicles in VANETs to protect their privacy while allowing secure and authenticated communication. PCs mask a vehicle's real identity by assigning it a temporary pseudonym, which helps prevent tracking while still verifying that messages come from legitimate sources. The SCMS system provides the vehicle with the necessary PCs to facilitate the pseudonym-changing process. PCs can be preloaded with varying periods for an extended time (e.g., one year) or obtained on-demand (e.g., daily), and each certificate has a validity period of five minutes.

Due to connectivity limitations, a vehicle may require certificates equivalent to three years in a complete deployment scenario, exceeding 300,000 certificates. Hence, vehicles have the ability to charge PCs online or offline. In online mode, vehicles can directly download PCs on demand using RSUs (Whyte et al., 2013). In offline mode, the PCA supplies all PCs to the vehicle regularly, necessitating ample storage capacity. However, this process is excessively costly due to the automotive-grade storage demands on the vehicle.

It should be emphasised that PCs have some unique features designed to enhance the security and privacy of vehicles and users in vehicular communications. These features play an essential role in maintaining the integrity and trustworthiness of the entire system. The following detail PCs unique features in SCMS:

- Pseudonymity: Pseudonym certificates lack real-world identifiers.
- Non-traceability: Vehicles receive multiple PCs, complicating traceability by allowing the use of different identities at separate times.
- Linkage Values: Embedded in PCs, these values facilitate efficient revocation.
- Issuing certificates for multiple periods: The SCMS issues PCs valid for extended durations in a single session, such as issuing weekly PCs collectively covering several years.
- Shuffle: Shuffling performed in the RA, is crucial in conjunction with Butterfly keys (Simplicio et al., 2018) to prevent PCA from deducing certificate-vehicle assignments, ensuring privacy against SCMS insiders.
- Continuous Generation: This ensures continuous certificate generation post-initial request, aiding vehicles in obtaining PCs swiftly when connected to the SCMS. It is particularly beneficial for scenarios requiring numerous certificates.
- Misbehaviour reporting: Enables vehicle reporting to detect and revoke misbehaving vehicles.
- On broadcast CRL: This feature allows easy identification of revoked certificates by adding certificate information to a CRL.

3.4.3 Misbehaviour Detection and Revocation

The process of misbehaviour detection and revocation involves identifying potential misbehaviour in the system, investigating suspicious activity, and revoking certificates of misbehaving vehicles upon confirmation. Misbehaving or defective vehicles transmit V2V messages containing false or misleading information (Nguyen et al., 2020). Vehicles need to disregard messages coming from misbehaving sources. Potentially misbehaving vehicles will be reported to the SCMS. The SCMS will then utilise misbehaviour detection algorithms to assess the situation and notify all participants regarding certificates that have become untrustworthy.

During the misbehaviour reporting process, vehicles submit reports to the MA. Although the exact format of a misbehaviour report is not yet fully defined, each report contains suspicious and alert-related Basic Safety Messages (BSM), linked PCs, a description of the misbehaviour type, as well as the reporter's PC and the corresponding signature from the time of report creation. Misbehaviour detection entails the MA being capable of discerning if multiple misbehaviour reports reference the exact vehicle (Van Der Heijden et al., 2018). This process also necessitates the MA to compile information for publication in a CRL to invalidate a vehicle's certificates. Furthermore, the MA must inform the RA with the necessary data to enable blacklisting, preventing the misbehaving vehicle from obtaining new certificates. The SCMS architecture requires collaboration among components to detect misbehaviour and implement a system of checks and balances:

- *Step 1:* The MA, PCA, and one of the LAs must collaborate to reconstruct linkage information.
- *Step 2:* The MA, PCA, RA, and both LAs must collaborate to generate revocation information for the CRL.
- *Step 3:* The MA, PCA, and RA must collaborate to identify the enrolment certificate of the misbehaving vehicle, which the RA will then include in its blacklist.

The MA conducts step 1 during the misbehaviour investigation to ascertain whether a vehicle or set of vehicles engaged in misbehaviour. Subsequently, after marking a vehicle as misbehaving, the MA proceeds with steps 2 and 3 during revocation to deduce the revocation information for the CRL and the enrolment certificate to be added to RA's internal blacklist.

The process starts when a certificate is flagged as compromised or otherwise untrusted. The MA responsible for SCMS revokes the certificate and publishes its details to the CRL. Linkage IDs and timing information are published on the CRL and distributed to revoke all PCs of a given vehicle over a given period. The list is then broadcast across the entire vehicular network so that all vehicles and infrastructure units know these revoked certificates. Upon connectivity, the updated CRL is periodically downloaded by vehicles from RSU or other secure distribution points. Every time a vehicle tries to communicate across the network, it validates certificates of the other parties against this CRL. This communication is blocked if the certificate appears on a list of compromised or unordered certificates, defending against possible influence from malicious and/or fraudulent sources out to communicate with other vehicles.

The current standard method for distributing CRLs involves sending them to each vehicle through various channels such as RSEs, cellular networks, satellite communications, or customer WiFi (Kamel et al., 2020). An alternative approach is implementing a collaborative distribution model outlined in a preliminary manner by Haas et al. (2011). In this model, specific vehicles are equipped with CRLs (via RSEs, cellular networks, or other methods) and transmitted to neighbouring vehicles as they pass by during their everyday operations. Vehicles that have received the CRLs become distributors, enabling comprehensive coverage of the entire system. This is essential to maintaining the integrity of V2V communications, allowing only trustworthy vehicles that are authenticated and authorised to participate in that network. However, the effectiveness of this process rests on a relatively current and properly circulated CRL; delays in updating or distributing an updated list can lead to security weaknesses that allow adversaries with revoked opinions to exploit the process.

3.4.4 SCMS Limitation with Disconnectivity

Despite its well-structured design, the SCMS faces several challenges. These issues are even pronounced in disconnected or rarely connected areas, where connectivity problems persist, complicating secure vehicular communications. In such situations, vehicles face difficulties communicating with the SCMS, leading to delays in certificate issuance and renewal. As a result, vehicles may end up using expired or invalid certificates, risking the security and trustworthiness of the messages they transmit. To illustrate, the implementation of SCMS in disconnected vehicular networks presents two primary challenges, as depicted in Figure 3.4. Firstly, maintaining and synchronizing the CRL is crucial for identifying the misbehaving vehicles. The CRL must be constantly updated and shared with all vehicles, a process that requires regular access to network infrastructure, typically via RSUs. This becomes problematic in areas with limited connectivity as the CRL grows with the number of misbehaving vehicles, necessitating frequent online updates.

Secondly, SCMS demands the use of multiple PCs for each vehicle to ensure message integrity and privacy. These PCs require regular updates as often as every five minutes to prevent message linkability, posing a significant challenge in disconnected areas. Vehicles must either preload a long-term supply of PCs or obtain them on demand, which requires substantial storage capacity or consistent online access, respectively (Brecht et al., 2018).

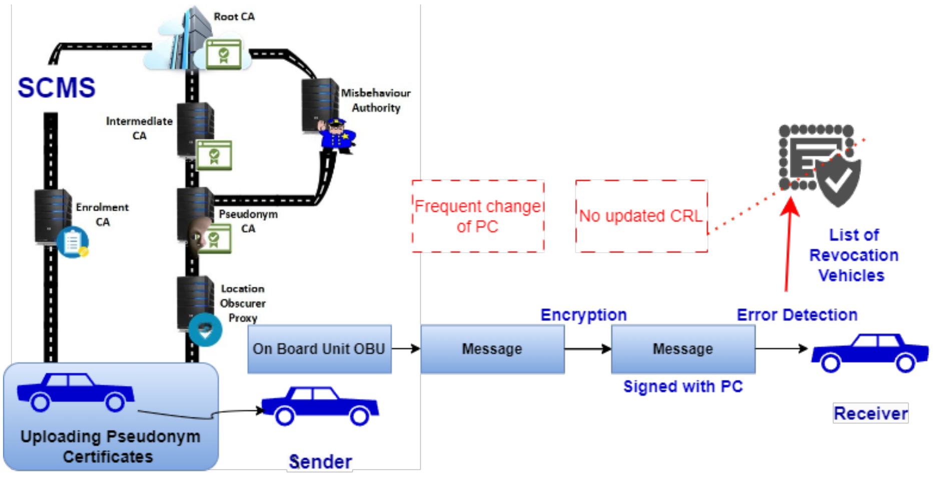


Figure 3.4: Challenges of SCMS in Disconnected Vehicular Network.

This dual challenge of effectively managing the CRL and PCs highlights the complexity of relying solely on SCMS in areas with limited network connectivity. Addressing SCMS challenges in disconnected areas, requires underscoring the importance of balancing several conflicting requirements, such as vehicle size, security, connectivity, and privacy.

- *PCs Privacy vs Size vs Connectivity:* PCs should be used temporarily for privacy reasons. Vehicles cannot store many PCs due to limited memory storage and its cost in a vehicle environment. On the other hand, in disconnected areas, vehicles cannot establish frequent connectivity to the SCMS to download new PCs on demand.

- *CRL Size and Retrospective Unlinkability:* The SCMS is responsible for revoking misbehaving or vehicles' PCs. However, putting all valid vehicle certificates on the CRL would make it very large. The system needs an efficient scheme to do the revocation without revealing the PCs used by the vehicle before it started misbehaving.

- *Balancing PCs Management and Sybil Attack Risks:* Each vehicle must periodically change its PCs for privacy concerns. One way to do this is to have many PCs, each valid one after another for a short period, resulting in many unused PCs. Another way is to have multiple PCs valid simultaneously for extended periods. However, this latter method increases the risk of a Sybil attack, where a single vehicle can masquerade as multiple vehicles.

3.5 Conclusion

The chapter discussed various security attacks and scenarios in vehicular communications. Then, it examined the security requirements and challenges for safeguarding vehicles and users in these communications. The chapter closed with a detailed discussion of the SCMS, highlighting its features as the foundational model extended to support advanced approaches. It also addresses issues surrounding PCs and CRL, particularly in disconnected areas, setting the stage for exploring complementary solutions in subsequent chapters.

Chapter 4

Security, Privacy, and Trust in V2V Networks

This chapter analyses the existing research on vehicular networks, emphasizing security issues in disconnected areas, PKI systems, and trust management mechanisms. It reviews foundational studies and recent advances on the background of a reputation-based trust enhancement model that draws on theories for generalizing these findings into novel application areas while also opening up avenues to address the limitations of existing work. This analysis sets the stage for positioning the work within the broader context of V2V security and reputation management.

4.1 Introduction

This chapter explores the state-of-the-art paradigms for forward security in vehicular networks. The discussion analyses the existing literature focusing on the security standards, trust systems, and reputation techniques suggested to address the unique challenges of V2V communications. It presents a detailed review of the literature related to V2V communication security, and details an analysis conducted on existing work pertaining to challenges facing current solutions. Although there has been a considerable body of research on security within V2V communications, the challenge of establishing trust in rural areas with limited connectivity is not been fully addressed by prior studies. This gap underscores the necessity for a novel scheme that utilises a reputation system to enrich trust among vehicles in disconnected environments.

4.2 V2V Studies in Disconnected Areas

Existing work on V2V communications in rural areas has focused either individually or collectively on the problems of sparse infrastructure, low population density, and limited connectivity. These studies investigated different approaches to address these challenges, such as modifying technologies already in wide use or creating entirely new protocols designed specifically for rural conditions. Despite significant progress, reliable communication in these areas is still critically important, especially when communication is disconnected. While *Section* 4.2.1 discusses studies that investigated V2V communications in such challenging conditions, *Section* 4.2.2 reviews the strategies for the deployment of RSUs in rural areas. This investigation is crucial to understand the recent V2V studies in disconnected areas.

4.2.1 V2V Connectivity in Rural Areas

Privacy, security, and trust preservation are crucial requirements in V2V communications. Recent studies discuss these requirements to cover various aspects of V2V communications, such as message dissemination strategies, routing protocols, security, privacy requirements, risks, and threats. Unfortunately, several gaps have not yet been addressed in challenging V2V scenarios, such as disconnectivity and communications in rural areas. Maintaining privacy, security, and trust in such a critical situation requires a robust system that balances these requirements to ensure a reliable and trustworthy V2V network.

Patel et al. (2015) conducted a survey comparing the performance of rural and urban distribution routing in V2V using proactive and reactive routing protocols. The primary focus is securing inter-vehicular environments through rural and urban simulations under Ad hoc OnDemand Distance Vector (AODV) and Destination-Sequenced Distance Vector (DSDV) routing protocols with variable vehicle speeds to study the effectiveness of their application. The results showed that AODV gave a higher packet delivery ratio value than DSDV. They also showed that the packet delivery ratio is inversely related to the end-to-end delay.

Nawaz and Sattar (2016) implemented a comparative analysis and performance evaluation of V2V protocols such as OLSR, AODV, and GRP. The study shows how these three routing protocols would perform in the two environments: urban and rural areas. The researchers carried out four test scenarios to analyse the performance of routing protocols to facilitate communication between vehicles using VANET safety applications, ensuring user safety. The performance of routing protocols changes significantly in different scenarios.

The results showed that AODV performed well in rural areas with low-congestion environments. A subsequent study by Yousaf and Majeed (2017) proposes an analysis of Quality of Service (QoS) with the AODV, DSDV, and DSRC protocols in rural and urban scenarios. The research used IEEE 802.11p for short-range communication and simulation in NS-2. DSRC performed better for packet drop and throughput in rural areas than AODV and DSDV; in the same instance, AODV performed well compared with DSRC in density regions.

The disconnectivity issue in remote locations has been investigated by Perumal et al. (2022). The study showed that Delay Tolerant Networks (DTNs) could be a potential low-cost solution to the issue of connecting vehicles in rural areas where infrastructure connectivity is not available. Researchers have worked on utilising DTNs to connect rural regions. Other schemes combined some safety applications with vehicle OBU systems to distribute personal health information (PHI) in rural environments (Jesús-Azabal et al., 2021; Koukis et al., 2024). These schemes provide network connectivity to rural areas using vehicles as relay nodes.

However, these schemes introduce a significant delay as DTNs depend on V2V data relay simply due to the mobility of vehicles, this would be especially problematic in rural areas where vehicle density is lower than average. When the delivery of information is time sensitive, this delay can be critical (Kuntke, 2024). Also, this reliance on vehicles as relay nodes may not be applicable or sustainable for other rural settings where RSU density is weak and vehicle access is limited as explained in the following section. These challenges highlight the need for more robust and adaptive solutions that can ensure reliable and secure connectivity in rural areas. The next section discusses various recent strategies for RSU placements.

4.2.2 RSU Deployment in Rural Areas

Roadside Units (RSUs) are pivotal in vehicular networks, enabling short-range wireless communications via IEEE 802.11p and a DSRC spectrum, essential for both data processing and internet connectivity (Liu et al., 2017). These units are integral in managing traffic data and facilitating connections with larger networks. RSUs further improve network performance through inter-unit communications. Vehicles within the same area relay information to each other, until one of them reaches the RSU, then, the message will be transmitted directly to the RSU. This occurs when direct communication to an RSU is not available with a single hop (Kosmopoulos et al., 2022). In addition, an RSU can directly communicate with another RSU forming a roadside unit-to-roadside unit (RSU 2 RSU) mode to verify safety messages and information sharing between vehicles (Azizi and Shokrollahi, 2024).

In this context, the level of RSU deployment becomes critical in VANETs operation at various statuses. High-density RSUs may boost communication efficiency and reduce delays for better network performance overall. However, this is unlikely in rural areas because of the costs and infrastructure needed to deploy RSUs, making the network operation challenging. These include the increasing reliance on V2V broadcast and greater vulnerability to disconnected scenarios. Consequently, any system design should consider the limited availability of RSUs in rural areas. To meet these needs, the investigation of strategies for RSU deployment is carried out to understand why rural areas have limited RSU infrastructure. The deployment of RSUs is clarified as the strategy of deciding the optimal locations of RSUs in a specific target region based on predefined parameters to achieve some requirements such as maximum connectivity coverage (Ullah et al., 2023), adequate connectivity, and low deployment cost.

Previous studies investigated advanced strategies for designing an efficient and optimised placement for RSUs. For example, the NP-hard combinatorial optimization challenge (Guerna and Bitam, 2019) demands strategies like Voronoi diagrams (Aurenhammer, 1991) and Constrained Delaunay Triangulation for optimal placement (Patil and Gokhale, 2013). In addition, Constrained Delaunay Triangulation (CDT) studied by Ghorai and Banerjee (2018), is an extension of CDT where some edges are constrained in the triangulation process. This is especially useful when there are natural barriers or roads that must be considered in the network layout. CDT can help to ensure that the network connectivity is maintained while considering these constraints.

Guerna et al. (2022) classified the RSU deployment strategies into two classifications: Dynamic and static deployment, as shown in Figure 4.1. In this Figure, dynamic deployment considers the utilization of both mobile and parked vehicles as RSUs, while static deployment considers fixed deployment for maximum coverage (Huo et al., 2024), geometric coverage (Liang et al., 2024), and optimal transmission time (Zhang and Hu, 2024) in the interests of optimizing RSU efficiency.

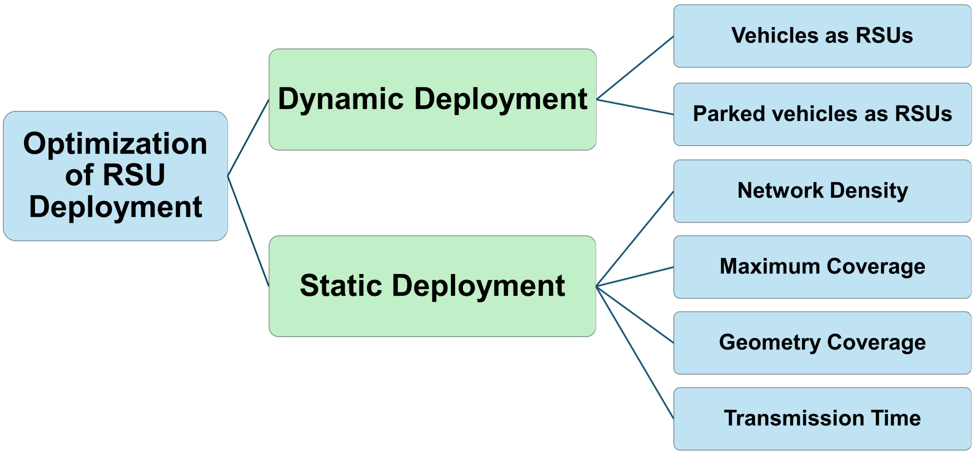


Figure 4.1: Taxonomy of RSU deployment.

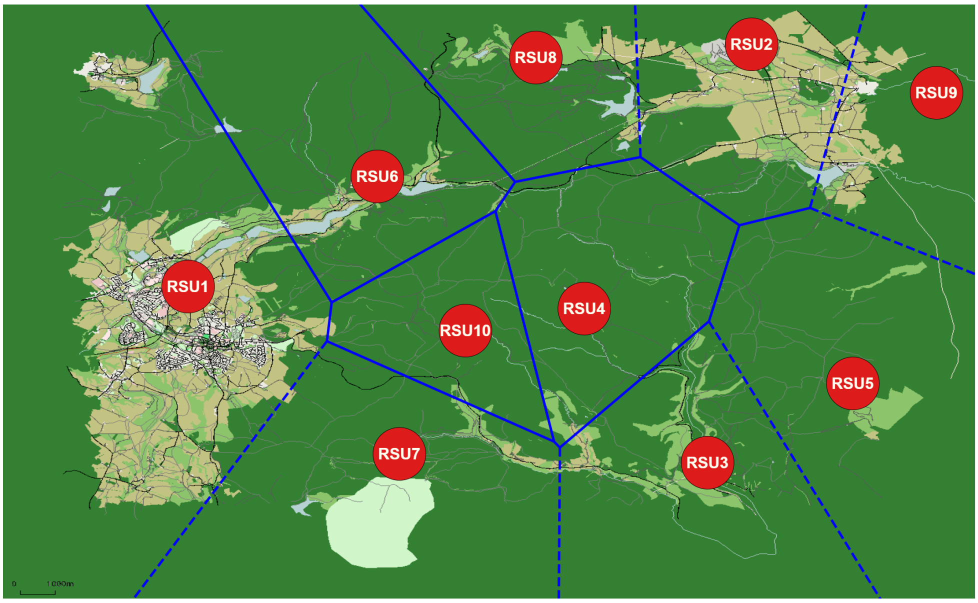


Figure 4.2: Strategic RSU Deployment Map for Optimal Coverage in a 10 km^2 Area of the Peak District.

A highly recommended RSU deployment strategy is to utilise Voronoi diagrams. This process involves partitioning the map into regions based on distances to a specified set of points (potential RSU locations). See Figure 4.2, which shows the map of the Peak District illustrating the implementation of the Voronoi diagrams in the selected study area.

Each point (RSU) would have a corresponding Voronoi cell such that any location within this cell is closer to that RSU than to any other RSU. It is useful for understanding and optimizing coverage. While the diagram demonstrates optimal RSU placement as a best-case scenario, it is unrealistic due to the associated deployment costs. This discussion is further extended in (*Chapter* 5), where the effect of low RSU deployment in Peak District is analysed and evaluated through simulations to highlight its impact on vehicular communication. This supports the need for the proposed reputation-based system for secure and reliable communication in the absence of RSUs.

4.3 Analysis of Certificate Management

Standards that manage vehicle certificates are crucial to authenticate the identity of each vehicle, maintain the integrity of the messages transmitted, and detect any misbehaviour in the network. Looking at existing methodologies and potential improvements, Section 4.3.1 provides an overview of studies that conducted PKI systems in vehicular communications. Additionally, the analysis covered the process of digital certificates and signatures, and examined the limitations of SCMS discussed in Section 4.3.2.

4.3.1 Public Key Infrastructure (PKI)

IEEE 1609.2 leverages the Public Key Infrastructure (PKI) system to manage security services and facilitate communication mechanisms within Wireless Access in Vehicular Environments (WAVE) units, making it applicable to vehicular communications (SAE International, 2021). According to Cui et al. (2018), a PKI system provides identification and message integrity, which could make it an optimal solution for the secure exchange of information in vehicular communications.

Joshi et al. (2017) designed an efficient technique based on an event trigger mechanism for vehicular communications, which uses a PKI-based signature to test the validity of broadcast beacon messages. Asghar et al. (2018) presented a PKI-based authentication protocol to enhance security by verifying vehicle identities. While this approach strengthens trust among vehicles, it needs more enhancements in terms of efficiency due to its computational demands of cryptographic processes, which results in latency responses that may cause undesirable consequences, especially during emergencies.

Another work by Liu et al. (2018) presented a privacy protection authentication scheme based on short-term local certificates with the limitation of certificate exchange requirements during an authentication process. Later, Jiang et al. (2022) presented a PKI-secured vehicle message broadcasting authentication protocol in VANETs. However, with the growth in the number of revoked certificates the complexity of identifying revoked vehicles from the CRL is relatively high. Additionally, the effectiveness of these schemes diminishes when applied to disconnected areas where vehicles have limited access to the RSUs. This results in creating complexity in obtaining a continuing set of certificates regularly.

Given that Identity-based Cryptography (IBC) is a means of mitigating the above certificate management problem, in 2015, He et al. (2015) presented an identity-based authentication scheme for V2V and V2I communication. In this scheme, a verification batch is added to manage multiple requests. However, this technique has some weaknesses, with the tradeoff of either exposing the original identity or privacy. In response, Cui et al. (2017) proposed a security privacy-preserving authentication algorithm based on a cuckoo filter. The underlying scheme using a cuckoo filter and binary search improved batch verification performance. Moreover, Qi and Gao (2020) presented an identity-based authentication scheme that uses pseudonyms to ensure privacy. However, IBC-based authentication schemes for vehicular communications have the defect of the key escrow issue (Ali et al., 2021).

It should be emphasised that designing an authentication protocol based on lightweight cryptography in Intelligent Transport Systems (ITS) is of great practical significance. A recent study by Liu et al. (2017) focusing on Lightweight V2I Authentication Protocol. Using a secret key, this protocol sets up a group of vehicles and RSUs from the Trusted Authority (TA), providing quick authentication. Another study by Xiong et al. (2018) proposed a lightweight V2I authentication scheme, referred to as VPCSM-0 and based on symmetric key cryptosystems, followed by Li et al. (2020) who further expanded the scheme's applicability. All these trust establishment mechanisms utilised the secret key that can be shared between the vehicle and RSU to authorize V2I communication after the successful authentication with the TA. However, the disadvantages of these methods are the requirements for secure channels, which may be impractical in low-infrastructure areas. Additionally, they lack non-repudiation, hindering accountability and traceability.

Tan et al. (2018) proposed a certificateless authentication scheme that provides better security; however, the computational overhead is high because they used the Chinese Remainder Theorem (CRT) and Elliptic Curve Cryptography(ECC). Lastly, Benyamina et al. (2019) proposed a lightweight authentication protocol leveraging the Message Authentication Code (MAC). However, its computational efficiency is limited, employing two classes for key updates. Li et al. (2020) proposed a hierarchical authentication protocol for vehicular communications based on Schnorr signatures and self-certified public keys.

Later, a novel scheme for the privacy-preserving authentication protocol was proposed by Zhang et al. (2021). It is based on bilinear pairings with batch authentication support for vehicles. Nath and Choudhury (2022) presented a privacy-preserving authentication system where authenticated vehicles can communicate based on the group key. In this context, some works available in the literature have shown the output as an anonymous authentication mechanism using bilinear pairings and a vehicle tracking scheme, along with a better approach to authenticating vehicles from different RSUs, which will be helpful and has a high importance for guidance for other research articles (Zhou et al., 2023).

Despite the advantages, these techniques face some limitations including high computational overhead, complex key management, and scalability challenges in dynamic networks, especially in rural areas where frequent group membership of vehicles changes, which requires an efficient distribution mechanism for real-time applications.

While the discussion of the existing studies related to the PKI in V2V communication provides a foundation of digital certificate management in vehicular networks, the insufficiency of existing solutions necessitates a focused analysis of related studies in the standard SCMS and certificates signature schemes. The next section explores studies that have implemented the SCMS standards, including those focused on pseudonym certificates, revocation schemes, and misbehaving managements. It also investigates recent efforts on digital certificate signatures.

4.3.2 Digital Certificates and Signatures

Previous studies investigated the SCMS-based security infrastructure and digital signatures to demonstrate their roles in secure, authenticated vehicle communication. SCMS deals with the proper issuance and revocation of digital certificates, which creates a basis for trustworthy V2V communications. Simultaneously, digital signatures provide message integrity and non-repudiation, essential for maintaining trust and accountability between vehicles. According to Cui et al. (2018); Xie et al. (2023), SCMS demonstrates its effectiveness as a promising solution for ensuring secure information exchange in V2V scenarios. Papadimitratos (2024) recommend that vehicles should be issued with 20 certificates weekly, which would be rotated every five minutes to increase privacy and make tracking difficult. This means that all 20 certificates will be used in 100 minutes, necessitating quick re-issuance and management. Although this method offers better scalability, it creates problems with privacy risks in the daily analysis of all certificates used by a vehicle. Gayathri et al. (2018) suggested the certificate signature idea without pairing for a high verification scale. A year later, Kumar et al. (2019) proposed a certificateless signature scheme for vehicle communications, which protects the vehicle's conditional privacy. However, both solutions have limitations in terms of functionality. As a result, researchers have started to investigate deeper into the functionality of aggregate signatures. In a study from Di and Wu (2022), and Yang et al. (2023), one of the sender's pseudonyms is used to sign and validate the broadcast messages. Hence, vehicles have to be periodically connected with the TA to obtain new pseudonyms in order to limit the effect of the linkage attack, which places significant pressure on TA. In addition, these studies lack implementation of safe transmission for a large V2V communication scale.

Cui et al. (2022) proposed a new certificate online/offline signcryption (COOSC) scheme that considers timestamp and pseudonyms mechanisms. However, this scheme does not count the issue of CRL updates in offline settings. In 2024, many variations of regular signature schemes have recently been proposed, including identity-based cryptography (IBC)-based pseudonyms (Tian et al., 2024) ring signatures (Bao et al., 2024), group signatures (Jayashree and Kumar, 2024), or blind signatures (Gao et al., 2024) to improve the security between vehicles in different scenarios.

Although earlier schemes provide significant advancements, they fail to tackle the core issue of balancing security, privacy, and trust in areas with limited connectivity. Addressing this issue requires more than relying solely on the SCMS system. The following section delves into exploring the trust management approaches in the literature to determine the best scheme to integrate reputation systems into V2V communications in rural areas to ensure a more reliable V2V network.

4.4 Trust and Reputation in Vehicular Networks

This section reviews the existing literature exploring trust and reputation as a means to enhance communication reliability and security in such an environment. *Section* 4.4.1 first provides an overview of VANET trust management in the literature leading to exploring related studies conducted on V2V trust systems. These systems establish trust among participating vehicles and ensure the integrity and confidentiality of exchanged messages, even in the absence of continuous network connectivity. *Section* 4.4.2 delves deeper by critically examines the reputation mechanisms proposed in the literature that are closely related to the themes explored in this study, highlighting their strengths and limitations to compare them later with the proposed reputation system. The analysis forms the foundation for the proposal of a novel scheme that uses reputation to address the unique communication challenges faced in rural areas during emergencies and attacks.

4.4.1 Evaluating Trust Mechanisms

Trust has been a primary concept in the relationship between entities in vehicular networks. An inaccurate degree of trust in VANET results in disuse (underreliance) and misuse (overreliance) of automation, which leads to decreased VANET performance and less AVs adoption (Hussain et al., 2020). In VANETs, trust is a key to coping with untrustworthy vehicles; it is described as a process that allows the receiving node (vehicle/ RSU) to determine whether the information from an arbitrary sender must be accepted or rejected.

Trust means the relationship between two nodes or vehicles that have been communicated to perform a specific task. One of these two is a trustor, which assumes that the other node will operate as expected, while the other is a trustee who maintains the trust by acting in the usual manner. If a vehicle consistently operates in an anticipated manner for whatever purpose, it is deemed trustworthy. When this idea of ”trust” is applied to VANETs, it implies that all network elements (users, RSUs, vehicles, infrastructure, sensors, and personal devices) act predictably, as though trustworthy information is communicated among them. According to Soleymani et al. (2021), ”Trust is a relation among various entities established based on past interactions' observations.”

Based on the nature of the network in which trust is formed, several related features in a highly dynamic VANET can be classified, as shown in Table 4.1. This classification of trust characteristics is adapted from Alalwany and Mahgoub (2024). For example, a vehicle on the highway may get an emergency message instructing it to change routes in an incident. Therefore, vehicles must issue a safety warning to other vehicles on the same highway. However, the reliability of this message must be verified based on different characters. Furthermore, this verification needs to be done while receiving the message before resending it to the neighbour vehicles again.

In this context, trust is built when the trustor believes that the trustee's skill is equal to or greater than the obstacles of an agreed task. For example, consider a scenario in which vehicles approach an accident. Vehicle A detects the accident first and broadcasts alert messages to other vehicles. For the alert to be trusted and acted upon, Vehicles B, C, and D must believe that Vehicle A (the trustee) has accurately detected and communicated the obstacle.

Table 4.1: Trust Features in Vehicular Networks.

Feature	**Description**
Dynamic	Trust variables must be dynamic, as they require regular computation and adjustment.
Composability	Trust information can be aggregated from multiple sources to form a unified opinion value.
Time dependent	Trust varies based on a vehicle's perception of another, which can change over time, leading to fluctuating trust levels.
Context dependent	Trust among two vehicles based on context. For instance, vehicle M can trust the vehicle N for forwarding data but not for receiving data.
Asymmetric	Two vehicles do not have to trust each other equally. For example, if a vehicle M trusts another vehicle N, vehicle N does not have to trust vehicle M.
Transitive	Trust is primarily transitive in VANETs. This means that if a vehicle P trusts a vehicle Q, and the vehicle Q trusts a vehicle S, then the vehicle P will also trust the vehicle S.
Direct/ Indirect	A direct trust is one in which the trust value is calculated based on the direct relationship between the trustor and the trustee. On the other hand, indirect trust is defined as a trust value generated from several neighbours' suggestions to the trustor.
Subjective/ Objective	When trust is calculated based on an individual's perception of the trustor, it is said to be subjective. However, when the trust is calculated using well-known parameters about the trustee entity, it is said to be objective.
Local/ global	When the trust value is solely available to the trustee and the trustor, it is said to be local means the value isn't transferable throughout the network. However, when each network entity has a unique trust value shared by all network entities, it is said to be global.

In a study by Morra et al. (2019), there are five main trust entities in VANETs. These entities work together to develop a network in terms of trust, as shown in Table 4.2.

Table 4.2: Trust Entities in Vehicular Networks.

Entity	**Description**
Trusted Users (TUs)	The user's role is essential for establishing trust in vehicles. If users fail to perform their tasks properly, the trust chain may be compromised.
Trusted Vehicle (TV)	Vehicles play a critical part in a network's many modes of communication. The most basic level of trust is to create security within the vehicle (Trusted Vehicle), and communications are carried out through trusted channels between vehicles (V2V)/ (V2I).
Trusted Medium	Users rely on information from vehicles or infrastructure, necessitating a trusted, secure channel for communication. Alternative channels can be used during attacks.
Trusted Route	Routing in VANETs involves hop-to-hop and hop-to-multi-hop communication, with dynamic configurations and open mediums, making it complex. Secure, trusted routing is essential for sending and receiving safety messages.
Trusted Applications	Users are served by both safety and non-safety applications, which make their journeys safer and more comfortable. Active safety apps, warning apps, and position-based routing require protection against attackers, and user trust grows as these applications complete their tasks correctly.

Shaikh and Alzahrani (2013) proposed a trust management scheme for the vehicular networks built upon three stages:

1. Receiver node calculates confidence value based on position closeness, time closeness, and position verification.
2. A trust value is computed for each message related to the same event.
3. The receiver node decides to acceptance of the message.

In this approach, a trust management model has been presented for ad-hoc networks that focuses on anonymity of identity. However, the proposed solution's position verification mechanism expected line-of-sight between the transmitter and the receiver, which is unrealistic. Furthermore, it lacks a mechanism for the revocation of malicious nodes. As a result, it is vulnerable to an on-off attack. Zhang et al. (2014) presented a trust management mechanism based on node voting. The more weight a node is assigned, the closer it is to an event. However, there is no way to determine which nodes are honest and malicious. Therefore, receiving and trusting messages from malicious nodes will be misleading and the consequences will negatively affect the performance of vehicles. It is also vulnerable to network attacks due to a revocation procedure for malicious nodes. Abbasi and Shahid Khan (2018) suggested a trust-based security model for VANET that confirms the reliability of received messages based on five factors. The five factors of Abbasi's model work together to raise the trust between nodes:

1. The *authentication* factor authenticates the messages between connecting vehicles during communication while preserving their privacy.
2. The *opinion* factor assesses the integrity of received messages.
3. The *credential* factor is concerned with presented credentials.
4. The *recommendation* factor oversees exchanging appreciations between vehicles.
5. The *alert* factor updates RSU and the TA about the misbehaving vehicle.

In 2018, a new security-aware routing method called VANSec was presented by Ahmed et al. (2018). In this technique, decision making checks the likeness index between received messages. As shown in Figure 4.3, trust models for VANETs can be categorised according to trustworthiness, establishment, and type of trust.

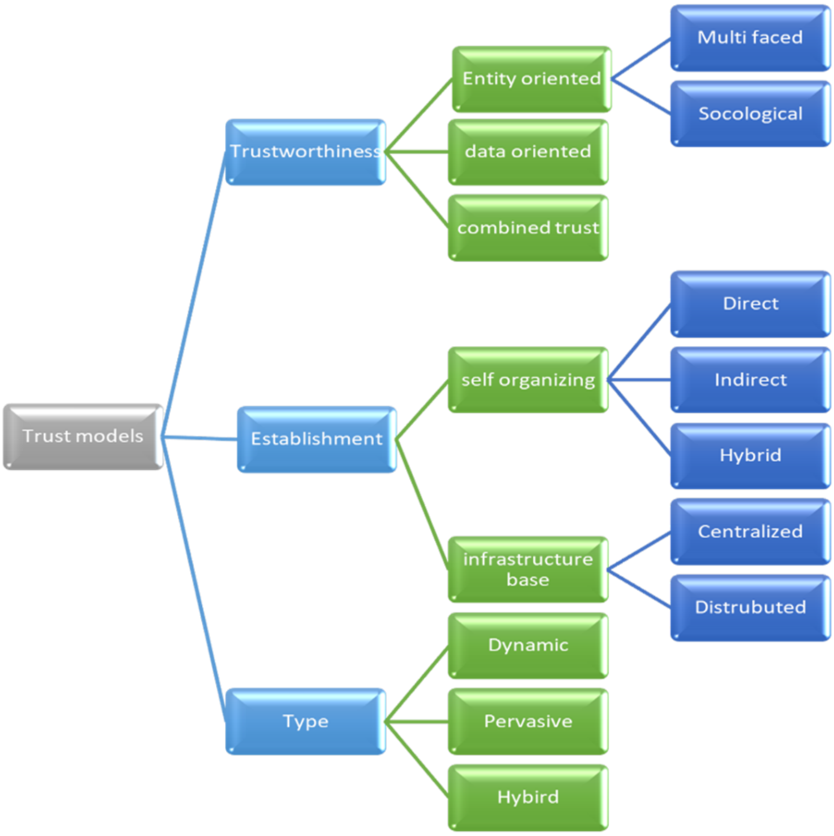


Figure 4.3: Security-Aware Routing Method VANSec.

The proposed trust model is based on a solid assumption: a vehicle typically circulates over the same path and at the same time of the day, which will help build history. However, Gao et al. (2021), argues for this non-realistic assumption. In Table 4.3, three factors are linked together to establish a suitable trust system as recommended by Zhang et al. (2022)

Table 4.3: Three Main Factors of the Trust System.

Factor	**Meaning**
Performance	The system observation of outcomes.
Process	The measurement of how the system works.
Purpose	The objectives of the system.

It is worth noting that some of these factors are directly or indirectly related to this work. Understanding these factors and how they work together is essential to designing an efficient trust mechanism in challenging V2V networks.

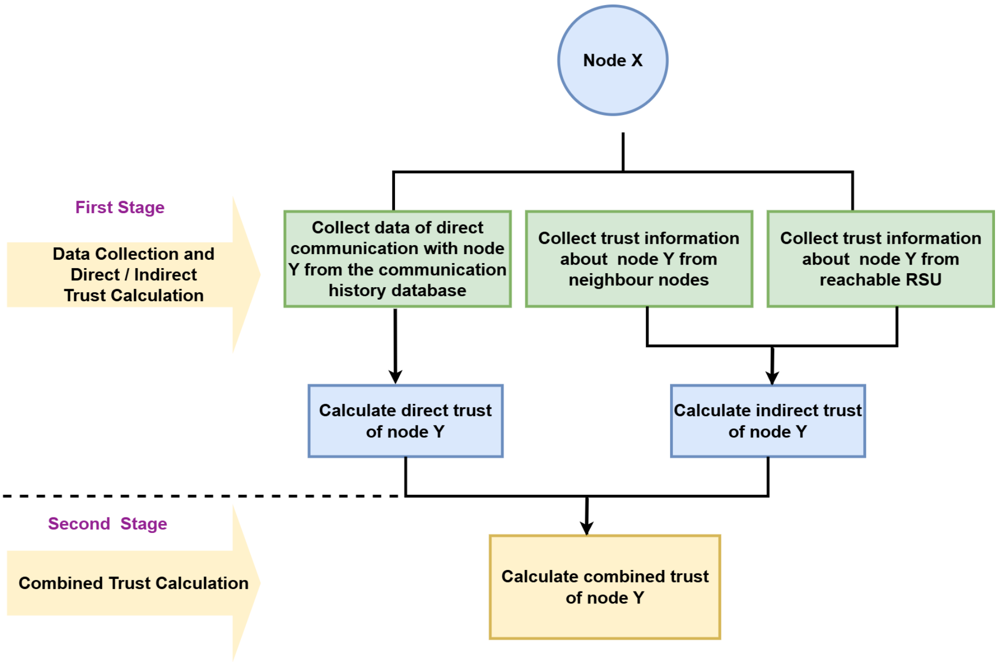

Node X
First Stage
Data Collection and Direct / Indirect Trust Calculation
Collect data of direct communication with node Y from the communication history database
Collect trust information about node Y from neighbour nodes
Collect trust information about node Y from reachable RSU
Calculate direct trust of node Y
Calculate indirect trust of node Y
Second Stage
Combined Trust Calculation
Calculate combined trust of node Y

Figure 4.4: Trust Establishment Process.

The trust establishment process proposed in the current research (Amari et al., 2023; AlMarshoud et al., 2024) assumed that vehicles X and Y have a trust relationship A (X,Y), see Figure 4.4. From the initiator's perspective, trust between these vehicles is established reliably when one vehicle trusts another to perform an expected function. If Vehicle X requests Vehicle Y to execute certain activities and Y completes these tasks successfully, Y is a trusted vehicle for X due to its positive behaviour. Vehicle X will improve the reputation value of Vehicle Y. As a result, the trust value grows with each activity a vehicle performs that the initiator expected.

In summary, while there is adequate research on trust management in the literature, existing work lacks a clear connection between trust and security, often neglecting reputation as a dynamic measure of trustworthiness. The research addresses these gaps by integrating trust into the secure SCMS standard, ensuring privacy, and then utilising reputation as a critical factor for evaluating and enhancing trust in dynamic and disconnected environments.

4.4.2 Exploration of Reputation Systems

Reputation means the mechanism for evaluating the behaviour of the vehicle over time, assigning scores based on their trustworthiness and reliability in the network (Agate et al., 2023). Reputation is a measure of trustworthiness derived from the collective evaluation of an entity's past behaviour or performance within a system, used to inform future interactions. It means the system's ability to score vehicles over time by calculating the behaviour of each vehicle in the network, assessing whether or not they are honest and accurate during sharing sessions. This not only detects malicious vehicles, but also encourages appropriate behaviour by awarding a higher trust score to a vehicle.

In this section, the most important characteristics of reputation systems and their application in VANETs are investigated as a basic procedure to secure network integrity. Moreover, the discussion explores various reputation schemes conducted in recent studies to maintain network integrity and security in both connected and disconnected areas. In recent years, there has been significant research interest in using reputation systems to minimize malicious behaviours for trustworthy V2V communications. To illustrate, reputation-based malicious vehicle identification systems have been devised and are gaining popularity to effectively deal with the threat of malicious nodes within the VANET. The receiver determines whether the sender is dangerous based on its reputation score and then finds a trusted communication path.

A key point to remember is that the V2V reputation system is categorised into centralised and decentralised models. The centralised reputation system uses a central authority to manage and evaluate trust, ensuring consistency but risking scalability and single-point failures. In contrast, distributed reputation system operates without dependence on infrastructure.

In this model, vehicles autonomously collect, maintain and update reputation scores in an ad hoc manner, enhancing scalability but introducing inconsistencies and vulnerability to malicious actors.

The centralised approach, pioneered by Li et al. (2012), revolves around a scheme that centrally distributes, updates, and stores vehicles' reputation scores. The study introduces a reputation announcement scheme for VANETs using Time Threshold to assess message reliability. They suggested the use of a reputation server as a reputation authority to generate reputation certificates; this approach is referred to as certified reputation, which was first proposed by Huynh et al. (2006). Samara and Alsalihy (2012) proposed a new reputation mechanism to identify malicious vehicles in V2V. This mechanism issues Valid Certificates (VCs) or Invalid Certificates (ICs) status for each vehicle and allows the vehicle to make a decision based on the sender's certificate status. Cui et al. (2019) proposed a centralised system for highways and urban roads, relying on a central Trusted Authority to calculate feedback scores from various vehicles and update the target's reputation. Moreover, Khan et al. (2020) proposed an incentive provision method in which the RSU updates the sender's reputation score based on observed actions validated by vehicles.

Cao et al. (2014) presented a decentralised approach, a multi-hop version that utilised the carry-and-forward method. The ideas aim to assess the message's reliability and the aggregation of reputation scores. In a similar way Katiyar et al. (2020) proposed a single-hop version that employed a single-hop reputation announcement. However, because messages and feedback are linked and not anonymous, these schemes do not provide enough privacy protection. As a result, an attacker can carry out a traceability attack and learn the path of a target vehicle.

Kerrache et al. (2016) presented a strategy for detecting malicious activities based on an adjustable detection threshold. In addition, defamation and harboring are addressed in reputation-based schemes by Gupta et al. (2018).

Tian et al. (2019) proposed a Vehicle Cash (Vcash) reputation framework to identify the denial of traffic service and to resolve the trustworthiness issue in the IoV application. In their work, every vehicle connects directly with the RSU to verify traffic events and then distributes the validated traffic event message. Furthermore, they take the idea of market trading and implement trade regulations to limit the propagation of malicious vehicles' misleading messages and encourage vehicles to participate in traffic event monitoring and verification. However, their work relies on RSUs, which are not available in the current case study. Moreover, their work targets a specific attacks in the network, and it does not consider some road issues and the different dynamic changes of VANETs. Gong et al. (2019) proposed a reputation scheme that assesses vehicle reliability based on their ability to forward packets without producing congestion. In addition, Wang and Yao (2019) focused on data trust and node trust simultaneously to identify malicious nodes.

Hussain et al. (2020) provided a trust and reputation architecture for VANETs, to manage the reputation of VANET. The goal of their study is to outline the reputation-based models' design specifications. The first objective of their concept is to identify malicious and selfish vehicles that could propagate false alarms. An Event Report (ER) is proposed by Raghu et al. (2020). In their work, when a vehicle detects an incident, it generates an ER that calculates the incident's reputation value. In this case, the incident information is reported only if it is above the threshold. El Sayed et al. (2020) developed a node reputation system to evaluate the reliability of vehicles and their messages. They grouped vehicles with similar mobility patterns that are close to each other into platoons to minimize propagation overhead.

Vaiana et al. (2021) introduced a hybrid approach that combines reputation values, proximity analysis, and severity assessment for evaluating accident reports. Their study shows the effectiveness of considering severity in reconciling conflicting messages and improving accident detection accuracy. The Dempster-Shafer trust model is applied to the aggregate evidence on misbehaving vehicles by Mosadegh and Farzaneh (2021). Vehicles are categorised as malicious if they exceed or violate the speed limit.

Two-pass validation and a two-phase transaction were included in the blockchain-based traffic event validation that Ahmed et al. (2022) suggested. They employed a consensus mechanism referred to as a Proof of Event, which employs two criteria. Vehicles send alerts to the RSU, which only takes them for a set amount of time. The RSU enters the notification phase once the number of alerts exceeds the first threshold. With the assistance of approaching vehicles, it can validate the alert, add it to the local blockchain, and use multi-hop transmissions to notify neighbouring vehicles about the incident. Once all RSUs have agreed that the incident is correct and have reviewed the supporting evidence and reports, the RSU notifies the other RSUs in the same zone. The occasion will be appended to the worldwide blockchain, including all local happenings. Vehicles for event verification can access the public global Blockchain. Unlike previous consensus methods, Proof of Event uses timestamps to select the block submitter, which reduces power usage. However, based on their proposal, the size of the global blockchain is enormous since it might encompass all the events in a very large geographic area, meaning that a significant number of events are likely to be added to the blockchain every day. Furthermore, their work lacks mutual authentication details. Out of all alert submitters, 40% of them are internal attackers, resulting in a 100% false event success rate.

Zhang et al. (2023) presented the trust model that employed an ID-based signature, a Hash Message Authentication Code (HMAC), and an RSA-based method to detect maliciously and incorporate massages. Kabbur and Murthy (2023) proposed a cooperative reputation scheme to detect and prevent false emergency messages, improving V2V reliability with minimal computational overhead.

Ke et al. (2024) suggested an elaborate reputation approach that considers the message's reliability and the sending vehicle's participation. Every vehicle is tracked, and based on the conduct of the watched vehicle, a trust score is assigned. The proximity-based approach prioritizes accident messages from the vehicle closest to the accident location (Gu et al., 2024). Their method improves accident detection accuracy and successfully reduces the influence of conflicting messages. However, rather than taking into account other factors, their approach focuses mostly on using proximity as a factor in dispute resolution.

In summary, reputation-based schemes have been proposed to enable trust between vehicles and evaluate the credibility of shared messages in V2V communication, limiting the consequences of conflicting accident reports in emergency scenarios. While these schemes have robust systems that improve reliability during V2V communications, they primarily focused on reputation systems in isolation without incorporating them with other critical factors, such as the PKI systems that ensure V2V privacy even in challenging networks. In addition to this vulnerability, Table 4.4 summarises the limitations of some proposed reputation schemes.

Table 4.4: Limitations in the Existing Reputation Schemes.

Limitation	**Description**
Reliance on Connectivity	Assumed a continuous connectivity.
High Communication Overhead	Required frequent exchange of reputation between vehicles costing high communication overhead.
Insufficient Threat Mitigation	Inadequately addresses threats like Sybil attacks or collusion.
Scalability Issues	Inefficient with large data volumes.
Limited Contextual Factors	Ignores contextual factors like location, time, or traffic conditions, affecting the accuracy.
Delayed Response	Not accurately timely update for real-time response regarding the current status of the network and new threats.
Privacy Concerns	Required extensive data sharing, raising privacy concerns.
Inflexibility	Lack adaptability to various emergencies or attacks, relying on fixed thresholds and rules that may not address all adversary behaviours.

The limitations in previous work necessitate innovative solutions that balance essential aspects: *Privacy, Security, and Trust.* It is fundamental to create a resilient reputation system that uses its features to adopt it in critical scenarios with limited connectivity to safeguard both vehicle functionality and confidentiality. The following section presents a critical discussion that links these three aspects before moving to the next chapter, which proposes the novel scheme.

4.5 Discussion: Reputation via Privacy, Security, and Trust

Enabling reputation systems in disconnected vehicular networks requires an analysis that combines privacy requirements, security protocols, and trust managements. This discussion brings together findings from three main themes identified in the literature review: V2V communications in disconnected environments, PKI mechanisms including SCMS, certificates, and digital signatures, as well as the trust management and reputation systems explored in the literature. The first analysis focused on V2V communications in rural areas which helped to understand the challenges and constraints of vehicles communicating without continuous network connectivity. This analysis led to an exploration of the related work in PKI systems such as SCMS, which are the main standards in ensuring authenticated and secure communication using certificates and digital signatures even when the network connectivity is untrustworthy.

Given this background, a study is introduced on the recent mechanisms that enable trust between vehicles in the absence of real-time connectivity, especially during emergencies, to ensure more reliable communication and coordination. Combining privacy, security, and trust in a balanced way is crucial to enabling robust and secure vehicle communication systems in isolated areas. The relationship between the requirements and the solutions for privacy, security, and trust in vehicular networks is shown in Figure 4.5.

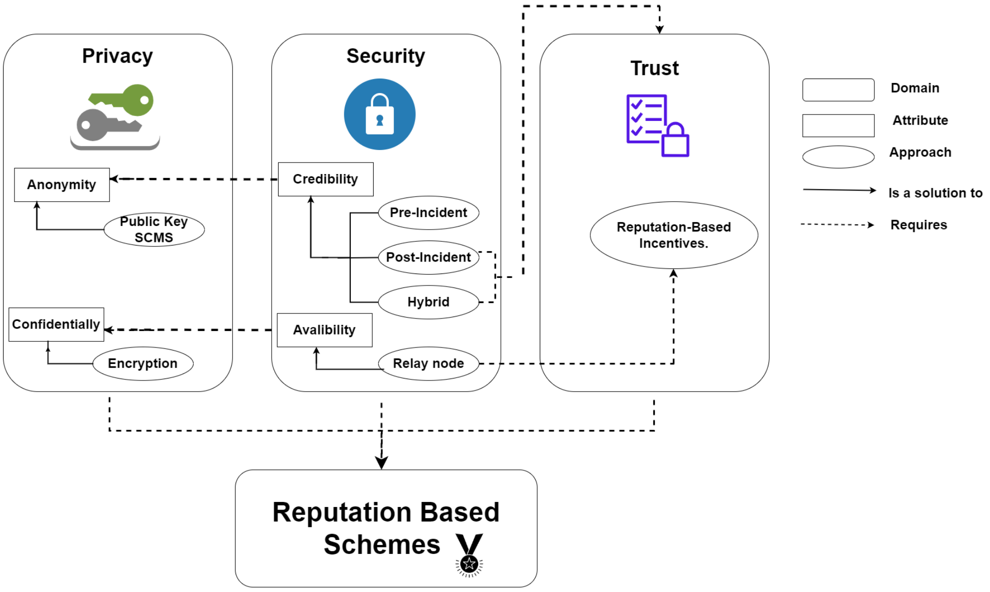


Figure 4.5: Relationship Between Privacy, Security, and Trust in V2V Communications.

- **Privacy**

  In VANETs, privacy is defined as limiting access privileges to nodes to view, exchange, or create messages to only specific nodes and allowing them to view the original identities of other nodes (AlMarshoud et al., 2024). There are two characteristics of privacy.

  - Anonymity: Is the ability to authenticate a node in a network without disclosing its true identity (Scalise et al., 2024). Public key cryptography (Zhou et al., 2023), which uses digital certificates and public/private key pairs for pseudonymous communications, is one of the most widely used methods for anonymity in VANETs. Key pairs and digital certificates are issued by a third-party trusted entity, or CA, for authentication.

  - Confidentiality: This indicates that a message's contents are private and that only authorised recipients need to have access to them. The goal of an eavesdropping attack is to compromise confidentiality by extracting data from unauthorized messages. Cryptographic techniques protect confidentiality but result in increased computational overhead, message size, and additional delay (Pandey et al., 2023).

  Acknowledging the necessity for privacy in V2V communications, the research explores the literature to understand the systems and standards that maintain V2V privacy during emergencies. This raises the question of *how to preserve vehicle privacy during communications in disconnected areas.* Based on the investigation, among various PKI systems, the SCMS PKI-based is the main standard to authenticate communications and preserve vehicle privacy due to its unique authorities, as explained in the previous (Chapter 3, *Section* 3.4). However, as explained later, the pseudonymous nature of V2V communication poses a challenge to integrating the reputation of vehicles.

- **Security**

  Secure V2V communication means that the network is protected from outside and inside threats and attacks. The main characteristics of VANET security include:

  - Credibility: Vehicles in VANET need to assess the credibility of a message before dissemination. The accuracy of a vehicle's initial message cannot always be guaranteed. This is because a malicious vehicle may have the following effects on a message's credibility:

    1. Generate an incorrect message.
    2. Validate an incorrect message.
    3. Reject a correct message.
    4. Collaborate with other malicious vehicles to execute any of the above actions.

    Three methods are used to evaluate a generated message's credibility:

    1. Pre-Incident: Where each vehicle has a trust rating that determines if the message it originated is true or false. The vehicle's message is disregarded if its trust rating drops below a predetermined level. This method can be cluster-based, with a cluster head managing trust ratings (Mahesh and Jawaligi, 2024), or centralised, with a TA storing trust ratings (Tiwari et al., 2024).
    2. Post-Incident: Where a message is verified based on the neighbouring vehicles' endorsements or votes above a certain threshold (Mittal, 2024).
    3. Hybrid Method: In which message credibility is assessed

    solely by trustworthy vehicles (Gao et al., 2021). The rate at which decisions are made, communication overhead, and the tolerance rate of malicious vehicles are the metrics used to assess a message validation or credibility strategy in vehicular communications.

  - Availability: The guarantee that a network will continue to function even when malicious vehicles are present. To ensure that all pertinent vehicles have access to the information in the event of an emergency on the road, a VANET must be able to autonomously distribute the message up to a predetermined number of hops, a targeted area or a time limit (Wu et al., 2024).

- **Trust**

  In VANETs, trust is employed to support security. For instance, communication credibility is assessed using trust ratings. Furthermore, vehicles are incentivised to collaborate and actively participate in message propagation through a gain in trust or reputation score. Since incentive distribution techniques suggest ways to update reputation or trust ratings, they are classified based on their trust management models. The primary incentive mechanism known as reputation-based solution employs trustworthiness measurement as a means of enforcing collaboration (Agate et al., 2023). A reputational threshold is established to differentiate between dishonest and truthful behaviour. Malicious behaviour is subject to a penalty plan. Typically, game theoretical analysis (Charoenchai and Siripongwutikorn, 2024) is employed to predict honest, malicious, or selfish activities of vehicles based on a predetermined incentive scheme.

  In addition to the effectiveness of motivating selfish vehicles to collaborate, incentive systems also deter malicious vehicles from trying to deceive others. In VANETs, it is critical to discourage malicious and selfish behaviour, as it could compromise the transmission of emergency messages and risk network safety.

Recognizing the importance of enabling trust among vehicles, the study reviewed related and recent systems in the literature, as indicated in (*Section* 4.4). The analysis shows that enabling trust in disconnected (offline) V2V communication requires a robust reputation scheme that works effectively with the SCMS to preserve vehicle privacy as well as to provide an adequate level of secure, authenticated, and reliable V2V communications.

4.6 Conclusion

The insights derived from the literature review and related work a significant gap: No study addresses the problem of enabling reliable communications between vehicles in limited infrastructure areas in emergencies. Addressing this gap consequently becomes the core focus of the remaining research, and the subsequent chapters each contribute different elements to a proposed solution.

The next Chapter introduces the novel reputation system that adds a layer of verification to the existing certification system for more accurate and reliable decisions against conflicting messages in disconnected areas. The novel solution allows the reputation to be used even when vehicles are pseudonymous without access to a central authority, resulting in improved effectiveness of offline V2V communication.

Chapter 5

A Pre-Signature Scheme for Enabling Vehicle-to-Vehicle Trust in Rural Areas

The literature review in the previous chapter highlighted several challenges faced by the existing mechanisms designed to enhance the reliability of communications between vehicles. This chapter proposes a novel solution called the (Pre-Signature) scheme that allows reputation to be used even when vehicles are pseudonymous without access to the infrastructure. Furthermore, the chapter evaluates the scheme in areas with low connectivity under different conditions. This approach significantly improves the effectiveness of V2V communication in areas with limited infrastructure.

5.1 Introduction

V2V communication systems have significant potential to improve road safety and traffic efficiency. Ensuring the authenticating of these communications is essential, especially in situations where infrastructure is lacking. At the same time, it is important to protect the privacy of the vehicles involved. The SCMS addresses this challenge by utilising pseudonym certificates. However, the pseudonymous nature of V2V communications complicates the integration of vehicle reputations.

In SCMS, the CRL plays a key role in identifying and blocking misbehaving vehicles from the network, as explained in (Chapter 3, *Section* 3.4). However, the synchronization of the CRL becomes imperative when vehicles gain access to the infrastructure, notably through *RSUs* (Shurrab et al., 2021; Li et al., 2012). This chapter proposes a novel solution that allows reputation to be used even when vehicles are pseudonymous and without access to the infrastructure. By extending SCMS with a reputation system, vehicles can securely retrieve and update their reputation from a dedicated server, resulting in improved effectiveness of offline V2V communication.

The innovative solution involves a new cryptographic primitive the *Pre-Signature*. It offers a more scalable and granular approach than CRLs by leveraging a reputation system. This system assesses vehicles based on their historical behaviour, providing a more nuanced view of reliability and trustworthiness. The focus is on effectively disseminating the Reputation Value (RV) for offline use while maintaining privacy. The goal is to develop a system to authenticate messages, which maintains privacy, works offline, and allows reputation to be used. This scheme enables an appropriate balance between reputation and pseudonymity in offline V2V communication. It increases message size by approximately a half kilobyte while ensuring efficient offline operation and secure communication, with minimal computational overhead for signing and verification operations.

Furthermore, the chapter addresses the unique challenges posed by sparse or irregular RSUs coverage in these areas, the study investigate the implications of such environmental factors on the integrity and reliability of V2V communication networks. Utilising the widely used SUMO traffic simulation tool, a real-world rural scenarios were created and simulated. An in-depth performance evaluation of the *Pre-Signature* scheme was conducted under the typical infrastructural limitations encountered in rural scenarios. Through a detailed 24-hour simulation, vehicle communications are analysed in rural areas under different conditions with limited RSU connectivity. This simulation is pivotal in demonstrating the practical effectiveness and feasibility of the *Pre-Signature* scheme, showing its capacity to bolster trust and reliability in challenging and disconnected regions.

The findings demonstrate the scheme's usefulness in scenarios with variable or constrained RSUs access. Furthermore, the relationships between the three variables, communication range, amount of RSUs, and degree of home-to-vehicle connectivity overnight, are studied, offering an exhaustive analysis of the determinants influencing V2V communication efficiency in rural contexts. The important findings are (1) that access to accurate Reputation Values increases with all three variables and (2) the necessity of Pre-Signatures decreases if the amount and range of RSUs increase to high numbers. Together, these findings imply that areas with a low degree of adoption of RSUs (typically rural areas) benefit the most from the proposed approach.

5.2 Proposed System Framework

In response to the identified challenges in disconnected vehicular areas, this section introduces the proposed framework. This framework, is designed to effectively manage trust and reputation in areas with limited or intermittent connectivity, thereby enhancing both security and operational efficiency. This section introduces the framework's main entities, then it explains the technical details of linking the RS to the V-PKI Architecture.

5.2.1 Framework Entities

As shown in Figure 5.1, a new entity, the Reputation Server (RS) is introduced, which provides the Reputation Value (RV). The RS will be linked to the SCMS. During the reputation retrieval process, the RV will be pre-signed by the RS; then, the RV will be sent to the requested vehicle to complete the signature and attach it to PCs.

The RS has the capability to associate a vehicle's identity with its corresponding RV, ensuring privacy while facilitating efficient reputation management. This approach allows the vehicle to maintain its anonymity while still benefiting from reputation-based services. However, the detailed feedback mechanism, which encompasses the historical information used to determine a specific RV, falls outside the scope of the current discussion and will be addressed in (*Chapter* 7).

The proposed framework provides a secure way of attaching a reputation value to PCs without compromising the privacy of the vehicles. Furthermore, it ensures that the RV is tamper-proof and can only be used by the vehicle. This approach also enables efficient reputation management, allowing fast retrieval of RVs from the RS.

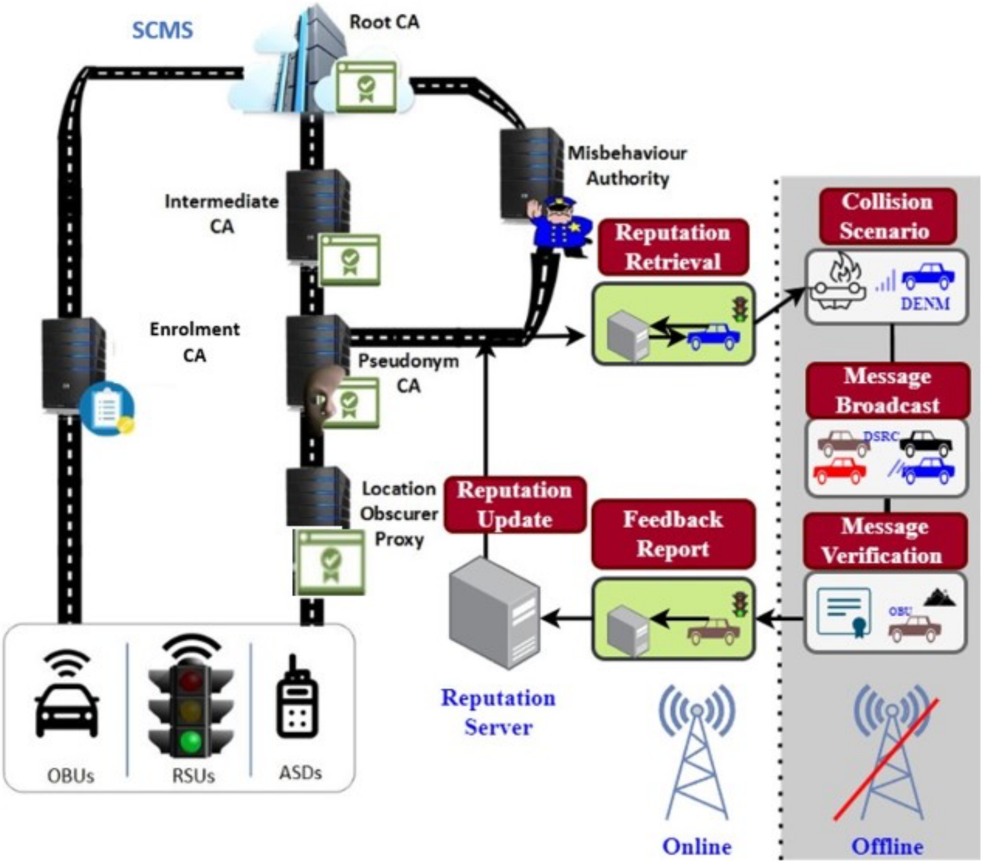


Figure 5.1: Proposed System Framework.

The roles and operations of the key entities in the proposed architecture are as follows:

- **Vehicles**

  In an offline setting, vehicles act as end users and communicate with neighbouring vehicles. Trust between vehicles is not assumed. Upon receiving a message, a vehicle assesses its reliability before proceeding. Vehicles are equipped with OBUs that facilitate wireless communication with neighbouring OBUs. Trusted hardware within the OBUs securely stores keys and handles cryptographic operations (Brecht et al., 2018).

- **Reputation Server**

  A centralised RS is introduced, which is considered a trusted authority. The RS's primary role is to manage the vehicle's reputation. This role comprises, gathering, and aggregating multiple reputation-related reports from vehicles to form an RV, then distributing a new RV to vehicles.

Vehicles can set up a secure channel with the RS using TLS (Krawczyk et al., 2013). The vehicle and the RS can exchange authentication credentials to establish a secure connection. Once the secure session is established, the vehicle can send its reputation requests to the server and receive responses securely. In addition, the secure channel ensures that the data exchanged between the vehicle and the server is not tampered with or accessed by malicious actors.

5.2.2 V-PKI Architecture with RS

IEEE 1609 and ETSI Intelligent Transport Systems (ITS) are two key standards that specify the vehicular communication. The former is for the US market and the latter is for the European market. Specifically from the security architecture perspective, IEEE 1609.2 (IEEE Vehicular Technology Society, 2016) and ETSI TS 102 940 (European Telecommunication Standard Institute ETSI40, 2021) define the Vehicular Public Key Infrastructure (V-PKI) system architecture, procedures, and messages. These V-PKI architectures are the building blocks for the security solution of V2X communication. Figure 5.2 illustrates the extension of the ETSI ITS V-PKI architecture (European Telecommunication Standard Institute ETSI40, 2021) by introducing the RS in this system.

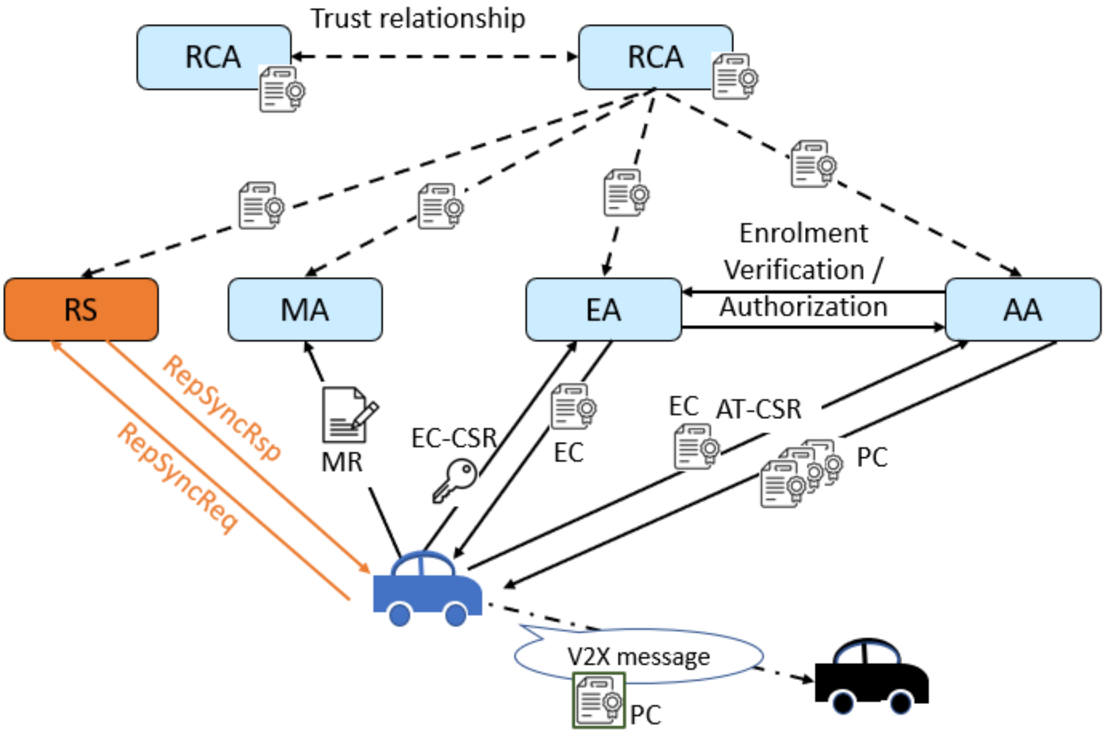


Figure 5.2: V-PKI Architecture with RS.

It should be noted that the incorporation of the RS into the process would necessitate updates to the related standards, namely IEEE 1609.2 (IEEE Vehicular Technology Society, 2016) and the related ETSI specifications for system architecture (TS 102 940) (European Telecommunication Standard Institute ETSI40, 2021) and protocol message formats and contents (TS 102 941) (European Telecommunication Standard Institute ETSI41, 2021). As shown in Figure 5.2, a new section should be created to capture the functional description of the RS.

Figure 5.3 illustrates the procedure in which a vehicle retrieves its RV from the RS.

Steps 1 and 2: When vehicle V contacts an RSU, it requests a reputation synchronization by sending a *RV_Sync_Request* message with the RS. The vehicle first encrypts its V_{ID} using its private key V_{SK} to the RSU ($V'_{ID} \leftarrow enc(V_{ID}, V_{SK})$). The RSU then forwards the vehicle's request to the RS.

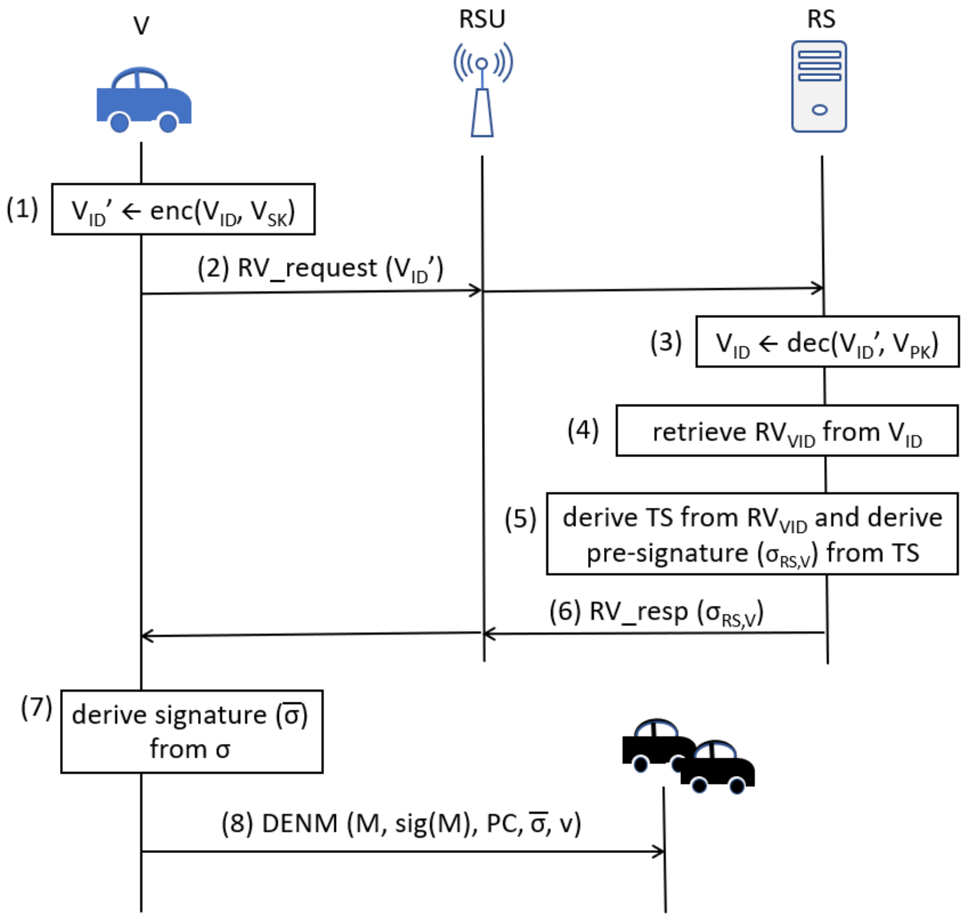

V
RSU
RS
(1) V_ID' ← enc(V_ID, V_SK)
(2) RV_request (V_ID')
(3) V_ID ← dec(V_ID', V_PK)
(4) retrieve RV_VID from V_ID
(5) derive TS from RV_VID and derive pre-signature (σ_RS,V) from TS
(6) RV_resp (σ_RS,V)
(7) derive signature (σ̄) from σ
(8) DENM (M, sig(M), PC, σ̄, v)

Figure 5.3: RV Retrieval.

Step 3: Upon receiving this request from the vehicle, the RS extracts the V_{ID} by decrypting the received value using the corresponding public key ($V_{ID} \leftarrow dec(V'_{ID}, V_{PK})$).

Steps 4 to 6: Using the V_{ID} as a key, the RS retrieves the RV value for this vehicle and computes the timestamp ($TS \leftarrow CT - round(7log_2(RV_{VID}))$). The RS derives the Pre-Signature of this TS value (σ) and returns it to the vehicle in the $RV\_Sync\_Response$ message.

Step 7: When the vehicle receives $RV\_Sync\_Response$ message, it uses the Pre-Signature value (σ) to complete the signature ($\bar{\sigma}$).

Step 8: The vehicle transmits DENM message to vehicles within its communication range ($DENM(M, sig(M), PC, \bar{\sigma}, v)$). The signature in this DENM message is generated using the Elliptic Curve Digital Signature Algorithm (ECDSA) according to clause 5.2 and 7.1.2 in ETSI TS 103 097 (European Telecommunication Standard Institute ETSI97, 2021).

Figure 5.4 illustrates the handling of Decentralised Environmental Notification Message (DENM) messages at the receiving vehicle when it receives the same message from multiple vehicles. This figure shows only two transmitting vehicles. However, in reality, it can be generalised to have n vehicles originating or relaying the same DENM message. DENM messages are explained in (*Chapter* 2, Section 2.3.3).

Step 1: Multiple vehicles $(V_{s1}, V_{s2}, ...)$ transmit (either originate or relay) the same DENM message $(M_{Vs1}, M_{Vs1}, ...)$. The generation of DENM message payload and its message signature are according to ETSI EN 302 637-2 (European Telecommunication Standard Institute ETSI72, 2019) and ETSI TS 103 097 (European Telecommunication Standard Institute ETSI97, 2021), respectively.

Step 2: The receiving vehicle (V_{rcv}) receives all messages from these vehicles. It verifies the message signature according to clause 5.2 and 7.1.2 in ETSI TS 103 097 (European Telecommunication Standard Institute ETSI97, 2021) and verifies the TS signature $(\bar{\sigma})$ from each vehicle. Based on the verified TS signature, it determines whether to accept or reject the received message from each transmitting vehicle.

Step 3: If the vehicle accepts the received message in the previous step, the receiving vehicles forwards the message.

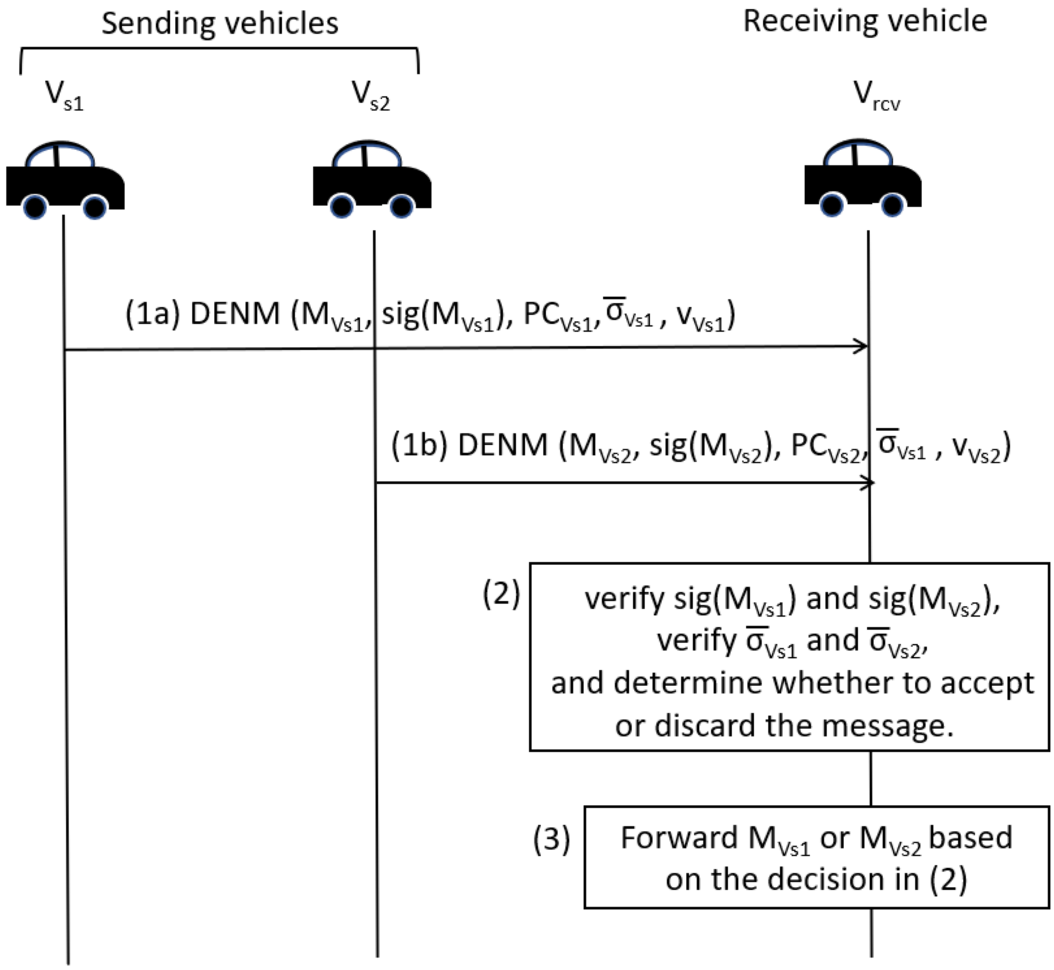

Sending vehicles
Receiving vehicle
V_{s1}
V_{s2}
V_{rcv}
(1a) DENM (M_{Vs1}, sig(M_{Vs1}), PC_{Vs1}, $\overline{\sigma}_{Vs1}$, v_{Vs1})
(1b) DENM (M_{Vs2}, sig(M_{Vs2}), PC_{Vs2}, $\overline{\sigma}_{Vs1}$, v_{Vs2})
(2)
verify sig(M_{Vs1}) and sig(M_{Vs2}), verify $\overline{\sigma}_{Vs1}$ and $\overline{\sigma}_{Vs2}$, and determine whether to accept or discard the message.
(3)
Forward M_{Vs1} or M_{Vs2} based on the decision in (2)

Figure 5.4: DENM Message Handling.

5.3 Novel Signature Scheme

In Security Credential Management System (SCMS), a vehicle's Pseudonym Certificates (PCs) allow other vehicles to be confident that the messages originate from that vehicle and have not been altered. Similarly, the RSU could supply vehicles with certificates with up-to-date reputation, but this creates a double challenge: (1) linking the reputation certificate to PCs without breaking pseudonymity; and (2) the reuse of the reputation certificate itself compromises privacy. An alternative approach would be that the RS regularly updates and signs the RV for each PC. However, this in turn poses a scalability issue as there are typically as many as 100,000 such PCs for each vehicle (Zeddini et al., 2022).

This section introduces a unique two-step signature scheme that addresses this privacy/scalability compromise. Many variations in regular signature schemes exist, to name a few: ring signatures (Fujisaki and Suzuki, 2007), group signatures (Jiang et al., 2020), delegatable signatures (Backes et al., 2016), blind signatures (Pointcheval and Stern, 2000), or proxy signatures (Ateniese and Hohenberger, 2005).

To the best of our knowledge, no existing variation addresses the specific challenge at hand. Thus, a new construction is introduced, the *Pre-Signature* scheme, which is described below. Although motivated by the specific needs highlighted above, the scheme may be of independent interest and is introduced in a generic context.

A *Pre-Signature* scheme involves three parties: an Issuer I, a Prover P, and a Verifier V. The Issuer I is considered honest. The Prover P and the Verifier V may behave maliciously.

Definition 5.1. *A* Pre-Signature *scheme $\mathcal{PS}$ consists of the following five algorithms:*

- $(pk, sk) = \text{keygen}(\ell)$*: I generates a public/private key pair with a security parameter (the security parameter ℓ is a variable determining the level of security in a cryptographic system. Increasing ℓ increases resistance against attacks, at the expense of increased computational and communication costs. In the specific context of the RSA-based implementation of the scheme introduced below, ℓ relates to the size of the RSA modulus.) ℓ, then keeps sk secret and distributes pk;*
- $(k, \{(b_i, v_i)\}_{i=1}^n) = \text{register}(P, n)$*: I registers a prover P by generating a* hidden key *k, and a set of n (*blinding key*,* verification code*) pairs. I keeps k secret and sends the set of blinding keys and associated verification codes $S_P \coloneqq \{(b_i, v_i)\}_{i=1}^n$ to P, and the verification codes on their own $\{v_i\}_{i=1}^n$ to V;*
- $\sigma = \text{pre-sign}(m, P)$*: I pre-signs a message m and sends it to P;*
- $\bar{\sigma} = \text{complete}(\sigma, b)$*: P chooses a blinding key b and completes a Pre-Signature σ, then sends the resulting completed signature $\bar{\sigma}$ it to V. In practice, the completed signature is also accompanied with an indicator for the verification code v corresponding to the chosen blinding key b;*
- $\text{verify}(\bar{\sigma}, m, v)$*: V verifies completed signature $\bar{\sigma}$ of message m using the associated verification code v.*

Figure 5.5 depicts the operations and interactions between the three parties in a Pre-Signature scheme.

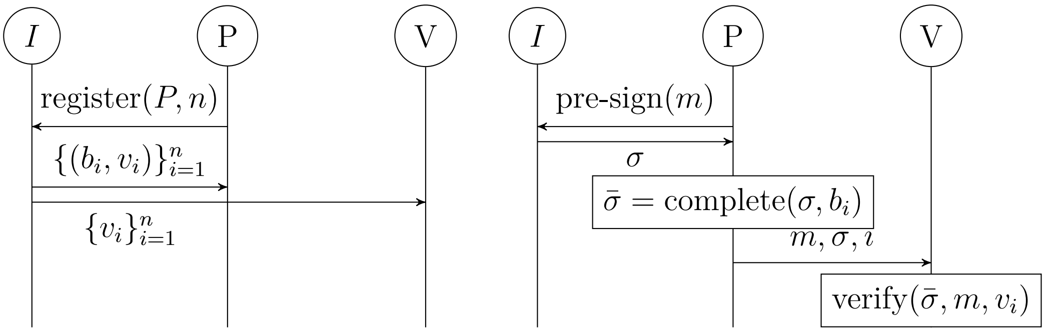


Figure 5.5: Sequence Diagram for Typical Operation of a Pre-Signature Scheme.

Definition 5.2. *The scheme $\mathcal{PS}$ is a secure Pre-Signature scheme if and only if it satisfies the following properties:*

Correctness *Completed signatures succeed verification iff valid, i.e., given* $(k, S_P) = \text{register}(P, n)$,

$$\text{verify}(\text{complete}(\text{pre-sign}(m, P), b), v) = \textit{True} \iff \exists (b, v) \in S_P.$$

In other words, given a message m, a valid Pre-Signature σ on m, and a valid completed signature $\overline{\sigma}$ on m and σ using b_i, the verification $\text{verify}(\overline{\sigma}, m, v_i)$ *succeeds if and only if (b_i, v_i) is a pair of blinding key, verification code in S_P.*

Unforgeability *For a malicious prover $\tilde{P}$, creating a valid completed signature for m^* using any $(b^*, v^*) \in S_{\tilde{P}}$ without* $\text{pre-sign}(m^*, \tilde{P})$ *is* hard*.*

Non-transferability *For a malicious prover $\tilde{P}$ knowing any* $\text{pre-sign}(m^*, \tilde{P})$ *and* $\text{pre-sign}(m^*, P' \neq \tilde{P})$*, creating a valid completed signature for m^* and a target $(b', v') \in S_{P'}$ is* hard*.*

Indistinguishability *Let $\sigma_0 = \text{pre-sign}(m_0, P_0)$, $\bar{\sigma}_0 = \text{complete}(\sigma_0, b_0)$, v_0 the associated verification code, and k_0, P_0's hidden key. Similarly for P_1, σ_1, $\bar{\sigma}_1$, b_1, v_1, and k_1. Given only pk, $(m_0, \bar{\sigma}_0, v_0)$ and*

$(m_1, \bar{\sigma}_1, v_1)$, determining whether $P_0 = P_1$ (or, equivalently, whether $k_0 = k_1$) is hard.

Below a construction of $\mathcal{PS}_{\text{RSA}}$ is proposed, a *Pre-Signature* scheme based on the RSA encryption/signature scheme:

- keygen: $pk = (e, N)$ and $sk = (d, N)$ with $(e, d, N) = \text{keygen}_{\text{RSA}}(\ell)$;
- register: k and $(b_i)_{i=1}^{n}$ are chosen at random in $\mathbb{Z}_N$, and $v_i = (kb_i)^e \pmod N$;
- pre-sign: $\sigma = h(m)^d k \pmod N$, with k the hidden key associated with P, and h a secure hash function;
- complete: $\bar{\sigma} = \sigma b \pmod N$;
- verify: returns True if and only if $\bar{\sigma}^e \equiv h(m)v \pmod N$.

Theorem 5.1. *$\mathcal{PS}_{RSA}$ is a secure Pre-Signature scheme.*

Proof. The four properties from Definition 5.2 are satisfied:

Correctness $\bar{\sigma}^e \equiv (\sigma b)^e \equiv (h(m)^d kb)^e \equiv h(m)(kb)^e \equiv h(m)v \pmod N$.

Unforgeability Without knowing σ^* or its own hidden key k, for $\tilde{P}$ to compute a valid completed signature $\bar{\sigma}^* \equiv (h(m^*)v^*)^d \pmod N$ would require computing the eth root of $h(m^*)v^*$. This reduces to the RSA problem.

Non-transferability Creating a completed signature for m^* and a target $(b', v') \in S_{P'}$ requires knowing the blinding key b' associated with the target verification code v'. The blinding key can be isolated by $\tilde{P}$ as $v'/v(b\sigma/\sigma')^e \equiv (k'b')^e/(kb)^e(bk/k')^e \equiv (b')^e \pmod N$ using known quantities. Computing b' from $v'/v(b\sigma/\sigma')^e \pmod N$ reduces to the RSA problem.

Indistinguishability The problem of determining r and s from $rs \pmod N$ (given r and s randomly distributed in $\mathbb{Z}_N$) solves integer factorization.

Under this reduction, since the blinding keys are randomly selected (in advance, by I), one cannot determine the blinding key or the Pre-Signature from a completed signature.

It follows that one cannot compute k_0^e from v_0 since b_0^e is secret (idem for k_1^e), and therefore distinguish k_0^e from k_1^e.

□

It is noted that since the hidden key k is static for a given Prover, a message m always has the same Pre-Signature. It is up to the Prover to protect its own privacy by changing the blinding key appropriately.

5.4 Reputation Decay Mechanism

This section introduces the concept of reputation decay in the proposed system for offline settings. Reputation values are designed to decrease over time in the absence of connectivity, ensuring the system mitigates the risk of outdated or unreliable reputation and maintains the integrity and reliability, even in disconnected environments.

5.4.1 Reputation Value

Reputation in V2V enhances communication reliability and effectiveness by identifying reliable messages and detecting vehicle misbehaviour (Samara, 2020). It does this in a more finegrained way than CRLs can. In addition, CRLs are not designed for offline settings. This work follows some established reputation assumptions in V2V (Cui et al., 2019; Li et al., 2012; Xu et al., 2020), estimating reliability based on feedback from communications.

It is assumed that a RS exists with a precise trust opinion. This trust opinion may simply be a single value or a more complex value, as in Subjective Logic (Cheng et al., 2019). Vehicles can request a RV, which is a numerical value between 0 and 1, derived from the RS's trust opinion. The message with the RV can be used in an offline setting to evidence its trustworthiness.

There is no mechanism to force vehicles to request an updated RV. A vehicle could request an RV when it is high, then misbehave, and simply not update the RV after it drops. This is a reputation lag attack (Sirur and Muller, 2019). To mitigate reputation lag, the RV, should decay. The study proposes a geometric decay rate with a half-life of a week, or about -9.43% per day. Taking the time units in days, after d days, an initial reputation of r_0 is decayed to $r = r_0 \cdot 2^{-d/7}$. This exponential decay pattern as explained in (ElSalamouny et al., 2009) ensures that reputation gradually diminishes over time. The decay is depicted in Figure 5.6.

To compute the current reputation using the formula, one would need to have the initial reputation and the timestamp of the message. However, as the decay is geometric, there exists an offset o, such that $r_0 \cdot 2^{-d/7} = 2^{-\frac{d+o}{7}}$, for all d. In fact, this occurs when $r_0 = 2^{-o/7}$ or $o = -7\log_2(r_0)$.

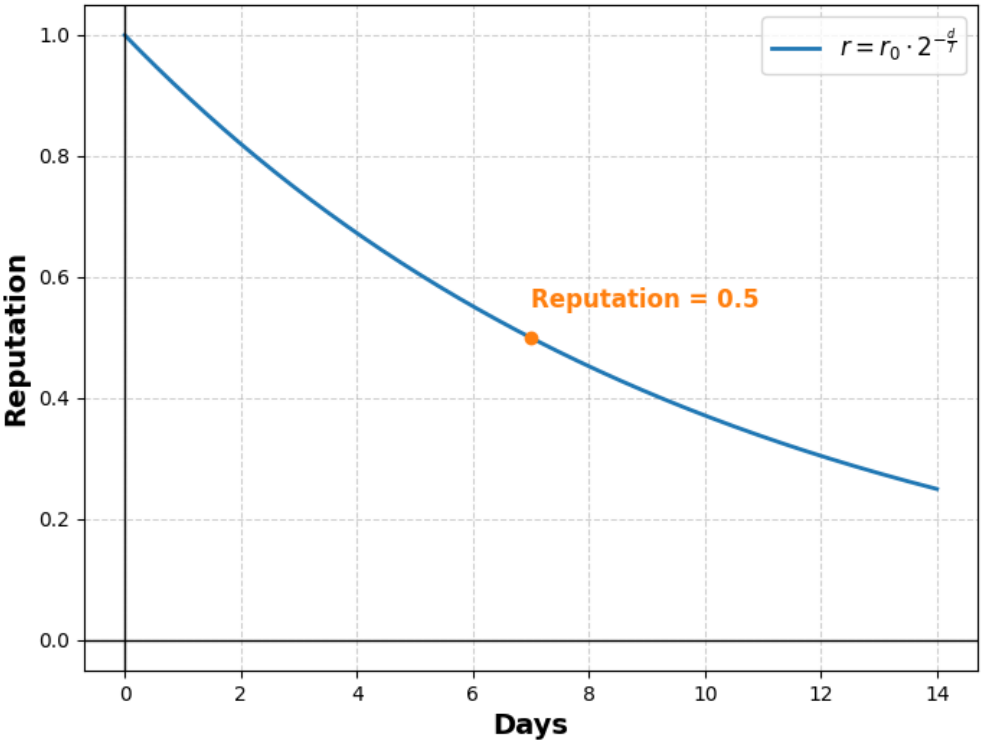


Figure 5.6: Decay of Reputation Over Time

Using this technique, the RV can be sent using only a timestamp – which is $7\log_2(r_0)$ days in the past – and implicitly have $r_0 = 1$. Hence, the value that will be sent is a timestamp TS. The entropy of the timestamp should be low.

After all, if someone notices that two timestamps are equal to the millisecond, then this may hint that its the same vehicle under a different pseudonym. Therefore, it is round TS to the nearest day. So, if today is T, then $TS = T - \text{round}(7\log_2(r_0))$. The vast majority of vehicles will be using a 'date corresponding to the last couple of days. The reputation value RV can be computed as $RV = 2^{-\frac{T-TS}{7}}$. This RV will approximately match the corresponding reputation value r_0 in the RS. As intended, the derived RV will decrease by about 10% per day, as T increases by 1 every day, giving us the desired half-life of 7 days.

Certainly, the scheme can be adjusted to decay faster or slower, or have more or less granular timestamps. In the employed decay system, the RV follows an exponential decay pattern, approaching zero without ever becoming negative. However, having a low reputation, such as $RS < 1/4$, does not have a particularly significant impact. Therefore, it is specified that honest vehicles should not use timestamps older than 14 days, as determined by $-7 \log_2(1/4) = 14$.

5.5 Privacy-Preserving V2V Communication

Vehicular communication relies on a secure network and privacy to enable safe interactions. This section covers essential V2V communication interaction, including DENM for hazard alerts. Additionally, the section discusses the three potential avenues for reducing privacy in the proposed system.

5.5.1 Vehicular Communication

The sender V_{send} wants to send the message M to the receiver V_{rcv}, using a specific PC. The message M follows the standards DENM and contains information such as location, time, type of message, and message contents (Marzouk et al., 2018). The DENM structure is depicted in Figure 5.7.

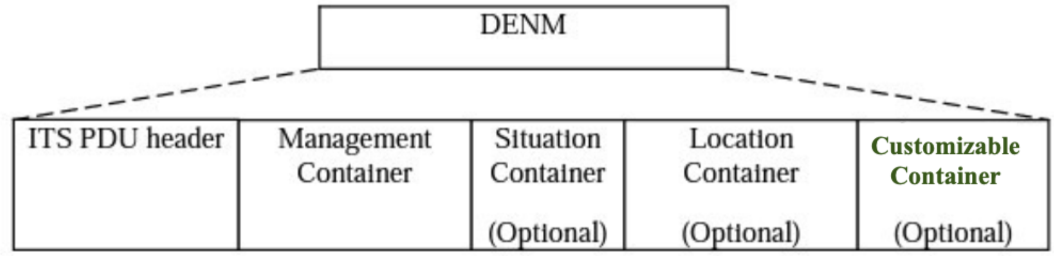

DENM
ITS PDU header
Management Container
Situation Container (Optional)
Location Container (Optional)
Customizable Container (Optional)

Figure 5.7: The Structure of a DENM Message.

The message needs to be signed with the private key PC_{SK}, so that the public key PC_{PK} on the certificate can verify it. An additional signature is further introduced to be included, based on the *Pre-Signature* scheme: V_{send} creates the completed signature $\bar{\sigma}_{RS,PC}(TS)$, using the blinding key PC_B and the stored pre-signature. For a message M, with pseudonym PC, and reputation RV, V_{send} needs to send:

$$(\sigma_{PC_{SK}}(M), PC, \bar{\sigma}_{RS,PC}(TS)) \tag{5.1}$$

As with normal DENM operation, the receiving vehicle V_{rcv} can verify that the certificate PC was issued by a trusted Pseudonym Certificate Authority (PCA). Additionally, it can verify that the owner of PC has correctly signed the message M, guaranteeing integrity and authentication w.r.t. the pseudonymous identity. In the proposed approach, vehicle V_{rcv} can furthermore verify (using the completed signature and the verification code on PC) that RS has provided evidence of a certain timestamp TS for vehicle V_{send}, and thus of reputation $RV = 2^{-\frac{T-TS}{7}}$ on day T.

In the context of the DENM system, Vehicle V_{send} generates the message M in DENM format. The DENM system is event-driven, and is meant to be used to identify safety issues (e.g., collision, obstacles, etc.). V_{send} sends M in hop-by-hop transmission format through the DSRC to neighbour vehicles in the same area. After receiving message M, the receiving vehicle V_{rcv} submits M to its OBU and verifies the message's reliability. Figure 5.8 shows the emergency communication in an offline scenario. The OBUs authenticate the message and the TS by verifying the source of the message and its integrity. Vehicle V_{rcv} receives many messages regarding the collision. In case of conflicting information, V_{rcv} has to decide which message is correct.

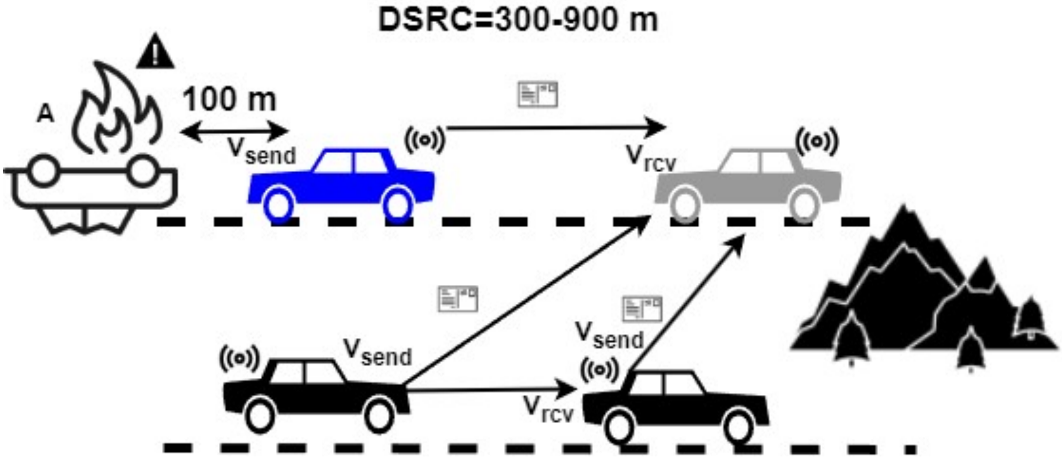


Figure 5.8: Emergency V2V Communication Scenario.

To support V_{rcv} in making the right decision, each sources reputation value can be used and compared. The RV provides additional information to help V_{rcv} make a more informed decision about the accurate message. By comparing the RV of the vehicles, V_{rcv} can determine which message is more likely to be accurate. If verified, V_{rcv} forwards M to its neighbour vehicles in the same area. They also interpret the message content and take appropriate safety measures. The actions to undertake, if any, may be influenced by the RV of the source. A comprehensive explanation of this process is presented in the next chapter.

5.5.2 Vehicle Privacy

The adoption of the proposed system introduces three potential avenues for reducing privacy: discernible patterns in verification codes, recognising that two completed signatures are based on the same pre-signature, and recognition of identical messages. However, verification codes are chosen at random, and the indistinguishability of completed signatures has been proven. Therefore, the only avenue in which privacy may be reduced, is by recognising the messages are identical. The message is a date TS within the last two weeks. This indicates the presence of 15 possible message values.

While matching TS values may hint that two PCs are from the same vehicle, there will be many vehicles using the same TS. The proposed scheme trades off reputation accuracy and privacy, but both the reputation accuracy is sufficiently high and the privacy is safeguarded, with the selected values. Overall, the scheme combines uses robust RSA encryption to enhance trustworthiness and resilience in V2V communication.

5.6 Operational Considerations

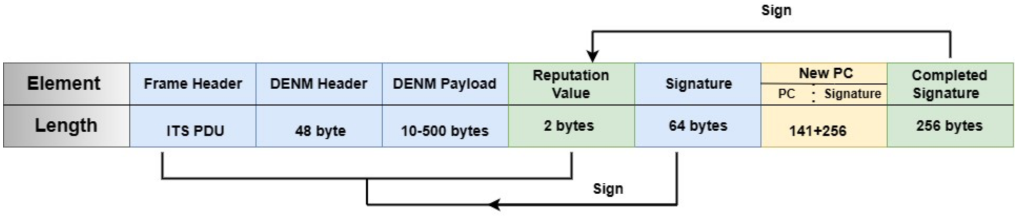
This section analyses the cost and overhead of the proposed scheme, specifically focusing on the added communication and signing/verification processes compared to existing systems.

5.6.1 RS to Vehicle

Efficient retrieval of RVs from the RS requires evaluating communication overhead. V2I scenarios use a specific message exchange protocol and employ DSRC with parameters like a 256-byte reputation response, 300-metre transmission range, 6 Mbps data rate, and one daily handshake. This ensures minimal overhead in bandwidth and latency, resulting in exceptionally efficient communication between vehicles and the RS.

5.6.2 V2V Communication

Within DENM messages, size considerations play a crucial role (European Telecommunication Standard Institute ETSI72, 2019). These messages are subject to a maximum size limit of 3,072 bytes, encompassing various components such as frame size, header size, payload size, and total message size. Figure 5.9 visually illustrates the integration of additional components introduced by the *Pre-Signature* scheme into the DENM.



Element	Frame Header	DENM Header	DENM Payload	Reputation Value	Signature	New PC PC : Signature	Completed Signature
Length	ITS PDU	48 byte	10-500 bytes	2 bytes	64 bytes	141+256	256 bytes

Figure 5.9: DENM Message Signed by*Pre-Signature.*

These components include updating the *PC* with a pre-signature, resulting in a size increase of 256 bytes, and signing the 2-byte *RV* with the completed signature, adding another 256 bytes. Therefore, the total size is increased by 514 bytes. The cumulative size increase amounts to approximately 0.50 kilobytes. While this is a substantial relative increase in size, it is important to consider the bandwidth capabilities of DSRC, which operates in the licensed 5.9 GHz band and is based on IEEE 802.11p (SAE International, 2020), where half a kilobyte is not substantial. The *Pre-Signature* scheme incurs minimal communication overhead compared to alternative signature schemes (Jayashree and Kumar, 2024; Bao et al., 2024), making it an effective solution for generating digital signatures in offline setting.

5.6.3 Computation Overhead

The *Pre-Signature* scheme demonstrates minimal communication overhead in terms of signing and verification operations. Verification operations are not significantly impacted due to the faster nature of RSA verification compared to ECDSA verification (Jansma and Arrendondo, 2004). This is attributed to the inherent computational efficiency of RSA, resulting in minimal overhead during the verification process. Similarly, the signing operations in the *Pre-Signature* scheme exhibit favourable performance characteristics.

The additional signature, referred to as the *completed* signature, involves a simple multiplication modulo N, which can be performed efficiently. As a consequence, the inclusion of the completion signature does not introduce substantial overhead during the signing process. Considering both signing and verification, the *Pre-Signature* scheme maintains an efficient computation overhead. This characteristic makes it well-suited for secure communication in offline environments, offering an optimal balance between cryptographic robustness and computational efficiency.

5.7 Establishing the Simulation Environment

This section discusses the simulation scenario, focusing on rural areas with varying RSU deployments. It introduces the simulation's core concept and explains the selection and configuration of the simulation tool. It also discusses RSU placement using Voronoi diagrams discussed in *(Chapter* 4) and details the setup of the experiments.

5.7.1 Simulation Concept Overview

This section presents a simulation focused on vehicular communication in the Peak District, as discussed in (*Chapter* 2), aiming to measure the impact of the proposed scheme in a rural scenario with limited RSUs density. The simulation, spanning a 24-h period, mimics real-world driving conditions to evaluate connectivity challenges due to sparse RSUs availability. By concentrating on the Peak District, the aim to explore situations where vehicles frequently find themselves outside the range of RSUs, necessitating reliance on direct communication with other vehicles. The simulation is intended to demonstrate the effectiveness of the proposed *Pre-Signature* scheme, particularly in rural settings where RSU support is limited.

Multiple 24-hour simulations are conducted under various conditions to assess how the scarcity of RSU infrastructure impacts communication reliability. These scenarios were evaluated with different RSU location availabilities. Additionally, various hypotheses for overnight connectivity were considered, accounting for the likelihood of vehicles connecting to the internet at night or in parking lots. This approach helped gauge the risk of being out of RSU range and its effect on communication reliability. The objective is to measure the effectiveness of the proposed solution in addressing these challenges in areas with sporadic connectivity.

5.7.2 Selection of the Simulation Tool

Simulation of Urban Mobility (SUMO) is a tool used worldwide for realistically simulating traffic and transport in urban environments (Sommer et al., 2011). While the tool is able to model multi-modal transport routes in urban environments, it is also able to simulate the simpler rural area, where vehicles alone are the primary mode of transportation. SUMO is the most appropriate state-of-the-art tool for generating realistic traffic for the conducted simulation. Utilising SUMO, real maps from OpenStreetMap can be imported, integrating them into the conducted simulations. This integration enables a comprehensive evaluation of vehicle communication, both with RSUs and among vehicles, across diverse rural and urban environments. See Figure 5.10.

The conducted simulation does not measure how the vehicles may respond to messages based on reputation. The behaviour of the individual vehicles on the road is independent of the current discussion, which will be addressed in the following chapter. This means that it is possible to record all vehicle behavior over a 24-h timespan, putting this into a single XML

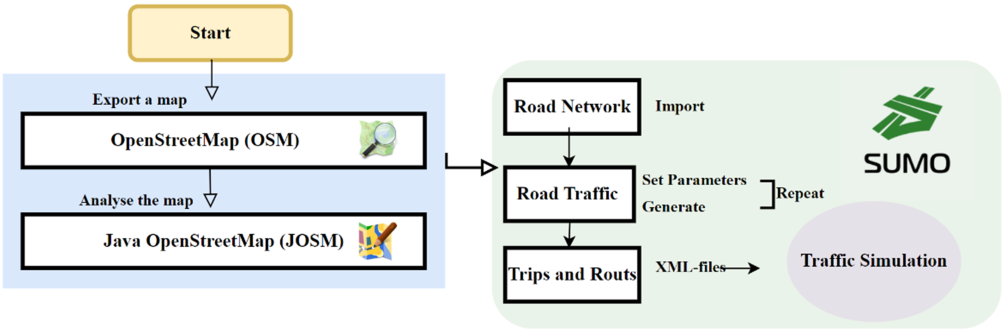


Figure 5.10: SUMO Architecture: Simulation Processes.

output file, and then have custom Python script analyse the output files to generate the measurements. The output of the Python scripts includes (xlsx) files, allowing further analysis of the measurements completed by the scripts using Excel and Python scripts.

5.7.3 RSU Placement Using Voronoi Diagrams

Voronoi diagrams can be used as a tool for strategically deploying RSUs in connected vehicular networks, as discussed in (Aurenhammer, 1991), this concept is discussed in details in (*Chapter* 4). To address the challenge of optimizing RSU placement, Voronoi diagrams are employed in a rural area. This geometric method divides the network area into convex polygons, each representing the coverage area of an individual RSU. Voronoi diagrams ensure that any point within a polygon is closer to its respective RSU than to any other, thereby maximizing network coverage efficiency.

Considering the possibility of 100 potential locations for 10 RSUs, a total of 1.73×10^{13} configurations were encountered. Figure 4.2 in (*Chapter* 4) visually illustrates this Voronoi-based approach, estimating the distribution of 10 RSUs within a 10 km square rural area, specifically, the Peak District.

In Figure 4.2, red dots denote RSU locations, and blue-bordered Voronoi cells delineate their unique coverage areas, each with a radius of approximately 900–1000 m. This strategic placement ensures efficient wireless communication coverage, facilitating seamless vehicle connectivity throughout the Peak District.

5.7.4 Experimental Setup

The simulation was conducted using SUMO to validate the proposed model utilizing IEEE 802.11p/1609.4 protocols. The simulation parameters are chosen to reflect the characteristics of a rural area like the Peak District and are detailed in Table 5.1. Key parameters include the network size, mobility model tailored to the Peak District's geography, vehicle communication standards, transmission range, and the simulation time, which spans a 24-h period.

In the simulation, V2R interactions are tracked at each time step (i.e., every second), meaning vehicles connect to RSUs whenever possible. V2V communications occur every 5 min; there is no universal standard for the frequency of exchanging, e.g., basic safety messages, and, moreover, occasional emergency messages are not sent on regular intervals but as an average; 5 min seems to be in the right order of magnitude for most applications. Importantly, all collected data throughout the simulation are systematically saved in an XML file format.

Table 5.1: Simulation Parameters.

Parameter	**Value**
Network size (km^2)	10
Mobility model	Peak District
Vehicle communication standard	(DSRC) IEEE 802.11 P
Road Type	Multiple ways
Transmission Range: R (m)	250
Simulation Time (s)	90,464
Total Number of vehicles	21,650
Number of vehicles per kilometre	10, 15, 20, 25, 30, 50
Vehicle Length	2.5
Roadside Units (RSU)	0, 1, 2, 3, 4, 5, 7, 10, 15
Overnight Connectivity Percentage	0% to 100%

The simulation mirrors real-time rural traffic conditions, with vehicles entering the network from various directions and lanes under different conditions. One key aspect is the vehicles' potential to pass within a 300 m or 900 m range of an RSU, in line with DSRC standards' minimum and maximum values. Upon passing an RSU within range, a vehicle's RV is updated, and the RSU pre-signed the RV before transmitting it to the targeted vehicle. Subsequently, these vehicles could encounter other vehicles within the same range and initiate communication by exchanging messages while providing an updated RV. This means that the recipient vehicle has evidence of the sender vehicle having an up-to-date and accurate reputation. This is referred to as a *'reputable communication'*.

This experiment assesses the influence of varying numbers of RSUs on rural vehicular communication systems. The conducted scenarios included setups with approximately 21,650 vehicles and different number of RSUs (0, 1, 2, 3, 4, 7, 10, and 15). The focus was on metrics such as total vehicle count, overall communications, reputable communications, the application of *Pre-Signature* schemes, overnight connectivity percentages, and the availability of online communication.

To comprehensively evaluate these metrics, a robust Dynamic Rural Area Connectivity scheme was developed. This scheme employs mathematical and computational methods to analyse vehicular communications in a rural setting:

- **Parameters**: Set RSU coordinates, communication ranges (`rangeRSU`, `rangeSRC`, e.g., 900), and `overnight,` e.g., (0.0).
- **Initialisation**: Vehicles have the 'reputable' status with probability `overnight`.
- **Data Processing**: Parse 'xml file' and initialize arrays for vehicle states and communication metrics.
- **Simulation Loop**: Iterate over time steps, updating vehicle distances to RSU; if a vehicle is within range of an RSU, its status is set 'reputable'. Every 300th timestep (every 5 min), loop through all pairs of vehicles; if a pair is within range of each other, 'total communications' is increased, and, if the sender has status reputable, then 'reputable communications' is increased. Finally, if the recipient was also in range of an RSU, then 'online communications' is increased.
- **Aggregation**: Compute total communication and engagement metrics from accumulated data.

This scheme enables the calculation and analysis of communication patterns based on data collected from a 24-h simulation conducted under various parameter settings. The aggregated data allow for answering various questions, including how effective the approach is in the scenario. Furthermore, this approach efficiently processed large datasets, allowing for a rapid assessment of dynamic communication patterns over time. This capability was crucial for understanding how different parameters, such as vehicle density and RSU placement, impact overall network connectivity and performance.

5.8 Simulation Results Discussion

This section discusses the key findings from the simulation of vehicular communication in the Peak District. The focus is on understanding the impact of the proposed approach within a rural setting, with limited availability of RSUs. The following analysis synthesizes the data collected from various 24-hour simulation scenarios, providing insights into the effectiveness of the proposed *Pre-Signature* scheme in enhancing connectivity under diverse conditions. The following figures derived from SUMO simulation GUI provide a visual representation of the communication scenarios enabled by the *Pre-Signature* scheme, illustrating its application and impact.

1. V2R Communication, Figure 5.11: Vehicles communicate with RSUs to update their RVs and obtain preliminary authentication credentials, ensuring network integrity within the RSU's service area.

2. Online V2V Communication, Figure 5.12: Vehicles within the RSU's range exchange information based on their RVs, guaranteeing the reliability of the communication.

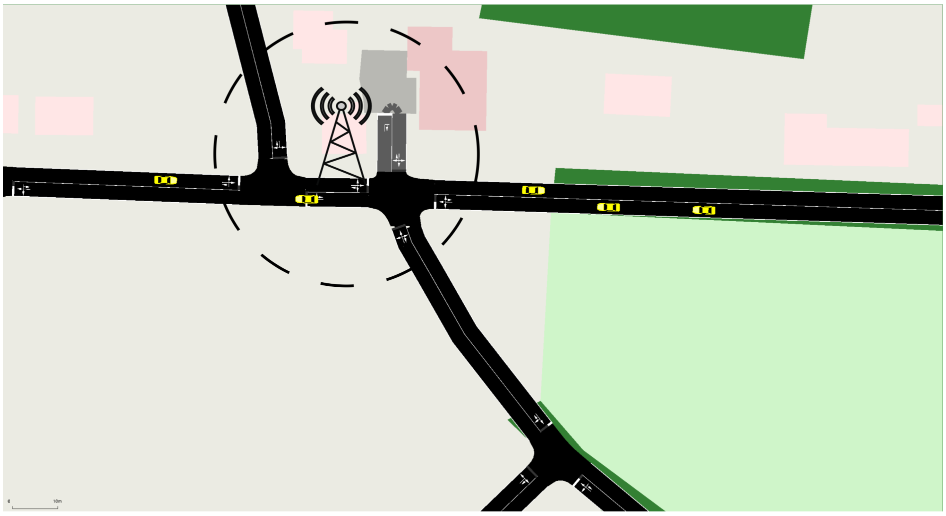


Figure 5.11: V2R Communication for Updating RV and Obtaining *Pre-Signature* from RSU.

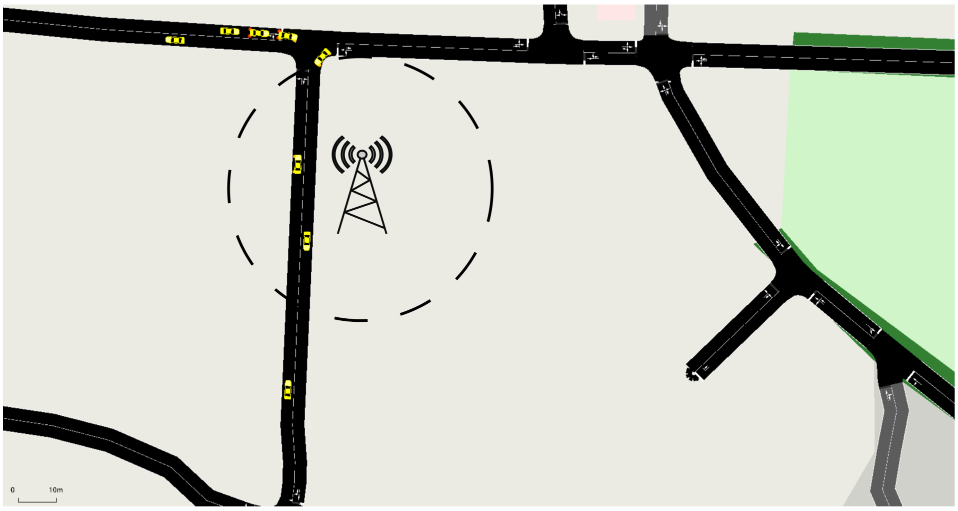


Figure 5.12: V2V Reputable Communication: Within RSU Range.

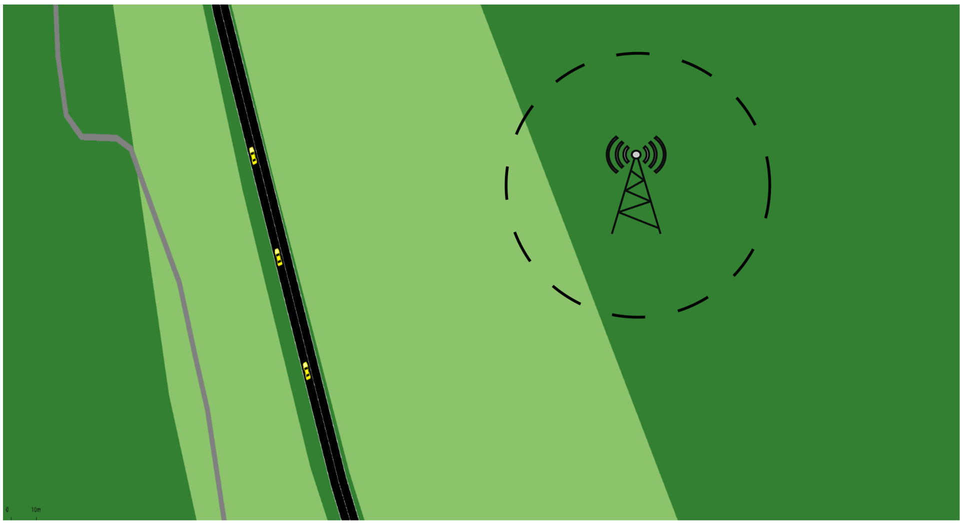


Figure 5.13: Offline V2V Reputable Communication: Outside RSU Range.

3. Offline V2V Communication, Figure 5.13: Vehicles communicate outside the RSU's range, utilising a Pre-Signature system to maintain dependable communication without RSU real-time supervision. Whether the communication has an up-to-date reputation available depends on whether the sender obtained a *Pre-Signature* prior.

These illustrative figures are a testament to the *Pre-Signature* scheme's critical role in enhancing vehicular network resilience, demonstrating the feasibility of reliable communication under varying RSU support conditions.

5.8.1 Key Metrics Analysed

The study conducted a comprehensive analysis of key factors to enhance the understanding of vehicular communication networks in rural areas:

- CV: The total number of vehicles is meticulously recorded at each second during the simulation.
- Vehicles with Pre-Signature (CPV): Special emphasis was placed on scenarios in which vehicles, upon encountering an RSU, received an updated RV or were accessible through overnight connectivity.
- TC: Indicates the total number of V2V communications.
- RC: The focus is on 'reputable communications', where vehicles with an updated RV successfully sent a message.
- ONRC: The extent of online communication availability was evaluated, signifying instances where vehicles with an RV communicated within the RSU's range. Here, reputation could be accessed via the

RSU, meaning that while the communication is reputable the proposed scheme was not necessary to accomplish this.

- ORC: A pivotal element of the research was 'offline reputable communications,' referring to the exchange of RVs between vehicles located outside the RSU's range. These represent communications where a valid up-to-date reputation is available thanks to the proposed scheme, where it otherwise would not be.

5.8.2 Evaluating RSU Availability and Overnight Connectivity

The analysis explored different scenarios of RSU availability and overnight connectivity percentages, from 0% (non-existent) to 100% (all vehicles have up-to-date Pre-Signatures at the start of day). These factors were assessed at every second of the simulation. This granular monitoring of parameters at one-second interval allowed us to gain detailed insights into the dynamics of vehicular communications across different RSU density scenarios.

Vehicle and Communications over Time with Limited Connectivity

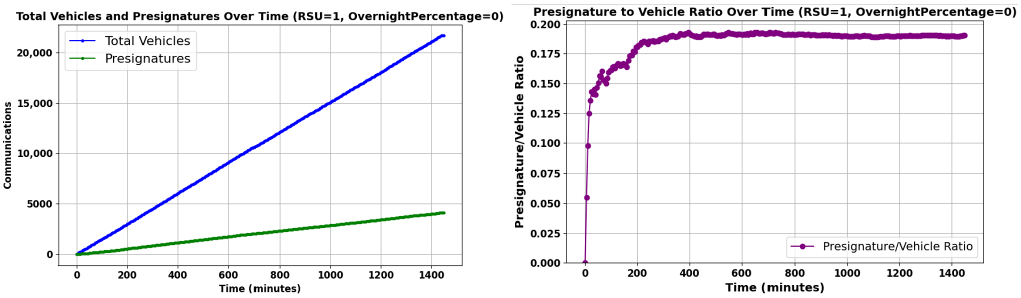


Figure 5.14: Vehicle Communication Activity Over Time with Limited Connectivity.

Figure 5.14 illustrates vehicle communication metrics over a 24-hour period under a scenario of low connectivity with one RSU. The left graph in Figure 5.14 shows a time series over 24-hour, charting the growth of CV and CPV (see Section 5.8.1 for abbreviations). The CV increases steadily, whereas the CPV count grows more slowly, which could be indicative of the limited presence of only one RSU. Despite the increasing number of vehicles, the ratio of CPV to CV remains constant, suggesting a uniform Pre-Signature distribution over time. This is further supported by the right graph, where the ratio between CV and CPV quickly converges to be constant.

An argument could be made that the fraction/number of vehicles with a *Pre-Signature* is not the quantity of interest as some vehicles may never/rarely communicate with other vehicles, and the presence of an up-to-date reputation is less relevant in such a case. One should not expect the presence of a *Pre-Signature* to be independent from the amount of communication a vehicle carries out as an isolated vehicle far from a town is less likely to have a *Pre-Signature* and is expected to communicate less—and vice versa for a vehicle in a town.

Figure 5.15 offers a view of various communication metrics over time. It encompasses the TC, depicted in blue, which represents the total num-

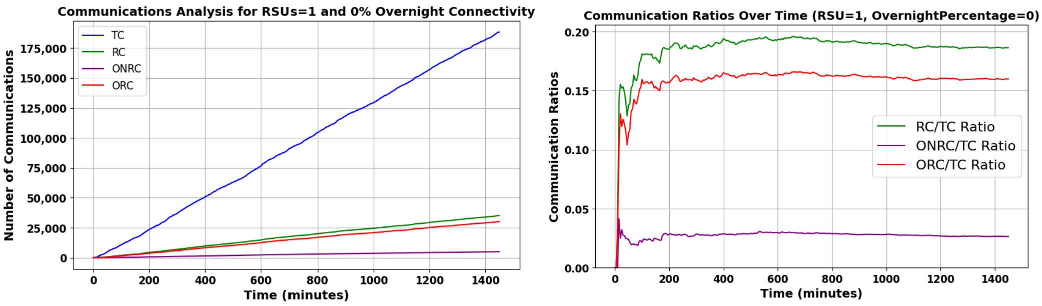


Figure 5.15: Time-Based Analysis of Communications Metrics for RSU 1 with 0% Overnight Connectivity.

ber of communications. The RC, in green, indicates those communications deemed reputable; the goal of any reputation system is to have this value as high as possible. The ONRC, shown in purple, highlights reputable communications accessible online. This is the performance of a naive reputation system without *Pre-Signatures*. Crucially, the offline reputable communications ORC shown in red represents the reputable communications conducted offline, which were enabled by the Pre-Signature scheme. This metric, underpinning the Pre-Signature scheme, emphasizes the strength and reliability of communications in offline settings. The steady or increasing trend of the red line on the graph underscores the robustness and adaptability of the Pre-Signature scheme, ensuring effective and secure transactions even without online connectivity. In the graph on the right, the line displays the ratio of RC to TC, providing a measure of communication quality relative to its quantity.

The ratios CPV:CV and RC:TC converge to similar values. However, there are two opposing effects at play. A vehicle could receive the Pre-Signature near the end of its lifetime, decreasing RC:TC relative to CPV:CV. Conversely, vehicles receiving Pre-Signatures are close to RSUs, which tend to be in busier areas, meaning a higher degree of communication for vehicles with a Pre-Signature. For the parameters chosen for this specific scenario, they happen to cancel out; this is not generally the case. It is important to understand the relationship between the parameters.

Evaluating RSU Deployment in Rural Areas

This section presents the outcomes of the simulation study focusing on RSU deployment in a rural setting, exemplified by the Peak District. The simulation explores the impact of RSU density on communication patterns within two different range scenarios—300 m, representing limited coverage, and 900 m, for extended coverage. The RSU deployment strategy commences with nothing and progressively increases the number of units, reflecting a realistic expansion towards 15 RSUs.

Figures 5.16–5.18 show an analysis of vehicular communication efficacy by RSU density and range (300–900 m). These figures offer insights into how different types of vehicular communications perform in scenarios where the overnight connectivity factor varies at 30%, 50%, and 70%, respectively. The analysis delineates three principal communication categories—Online Available, Reputable, and Offline Reputable. The RSU densities are varied to simulate different deployment stages:

- 0 RSUs: Represents an absence of RSU presence.
- 1 RSU: Indicates a very low RSU density, with minimal coverage.
- 3 RSUs: Depicts a low RSU density, offering limited communication capabilities.
- 5 RSUs: Corresponds to a medium RSU density, reflecting an improving infrastructure.
- 7 RSUs: Demonstrates a high RSU density, nearing effective coverage.
- 15 RSUs: Signifies a very high RSU density, with a robust communication network.

Figures 5.16–5.18 (left) show that, for the 300 m range, RSU density has a small impact on online communications, while the number of reputable communications generally increases with increasing RSUs.

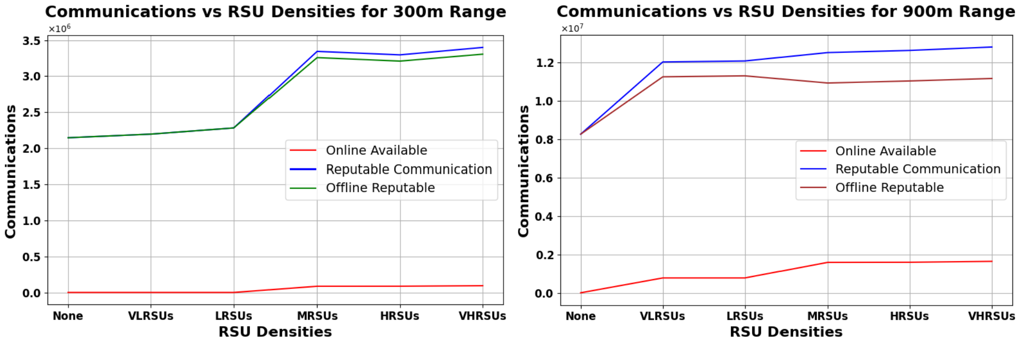


Figure 5.16: Analysis of Vehicular Communication Efficacy under 30% Overnight Connectivity Across Various RSU Densities, with Comparisons at 300 m Range **(Left)** and 900 m Range **(Right)**.

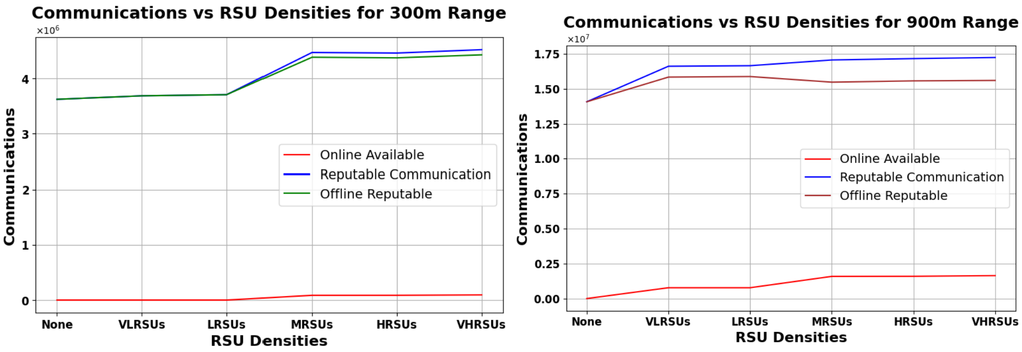


Figure 5.17: Analysis of Vehicular Communication Efficacy under 50% Overnight Connectivity Across Various RSU Densities, with Comparisons at 300 m Range **(Left)** and 900 m Range **(Right)**.

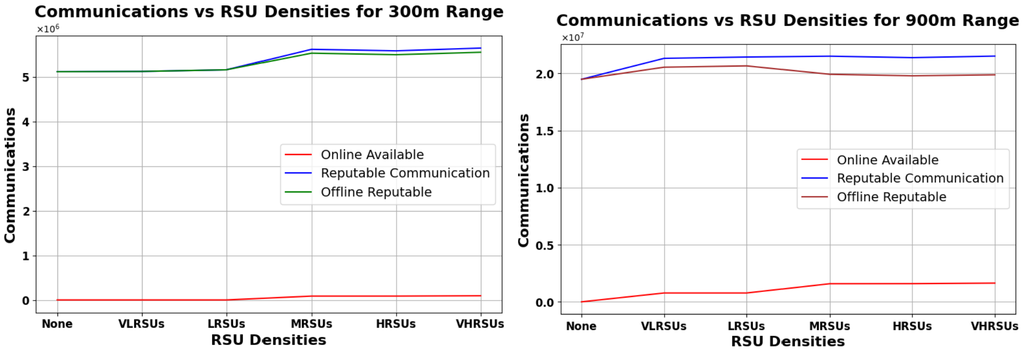


Figure 5.18: Analysis of Vehicular Communication Efficacy under 70% Overnight Connectivity Across Various RSU Densities, with Comparisons at 300 m Range **(Left)** and 900 m Range **(Right)**.

At the 900 m range (right graphs), both online and reputable communications experience a slight enhancement at lower RSU densities with diminishing gains as density increases. The line for ORC is fairly close to

RC in all the graphs, meaning that the proposed scheme is the primary contributor to the availability of reputation in the rural scenario. In Figure 5.18 (right), it can be observed that ORC decreasing a bit, suggesting a unimodal curve, where a very high RSU density allows for increasingly more reputation to be available online, diminishing the need for the proposed scheme. Note that, in an urban scenario, the density of RSUs may be orders of magnitude higher, allowing the ONRC to overtake the ORC—which would imply that the proposed scheme has less benefit in such an environment. However, as long as ORC is larger than zero, the impact is positive (and if zero, the impact is nil).

Overall, RSU impact is more significant at lower densities and diminishes with greater range and density. The analysis indicates that deploying even a single RSU can significantly enhance communication patterns in rural areas. As RSU density increases, the efficiency of the proposed *Pre-Signature* scheme improves, particularly within the RSU range. This improvement is evidenced by the increase in reputable communications, both online and offline. However, the most notable enhancement is observed in the online reputable communications, highlighting the benefits of RSU proximity.

Notably, even in the absence of RSU presence ('None'), the graph denotes a substantial count of ORC. This phenomenon accentuates the Pre-Signature scheme's strength in fostering trust and reliability in vehicular communications devoid of centralised infrastructure support. The scheme's resilience is further corroborated by the consistent level of ORC observed across all RSU densities, which is critical for the autonomous management of Reputation Values.

These findings articulate the *Pre-Signature* scheme's critical role in enhancing vehicular network resilience, particularly under the stringent different cases of overnight connectivity. This resilience ensures reliable communication channels in scenarios where RSU deployment is either sparse or entirely absent, which is a common challenge in rural and underserved regions.

Analysis of Communication Types over Overnight Percentage

Figures 5.19 and 5.20 offer a visual analysis of how overnight connectivity percentages affect communication patterns for vehicles in rural areas, where internet access is often conditional on being near home networks or designated parking lot hotspots.

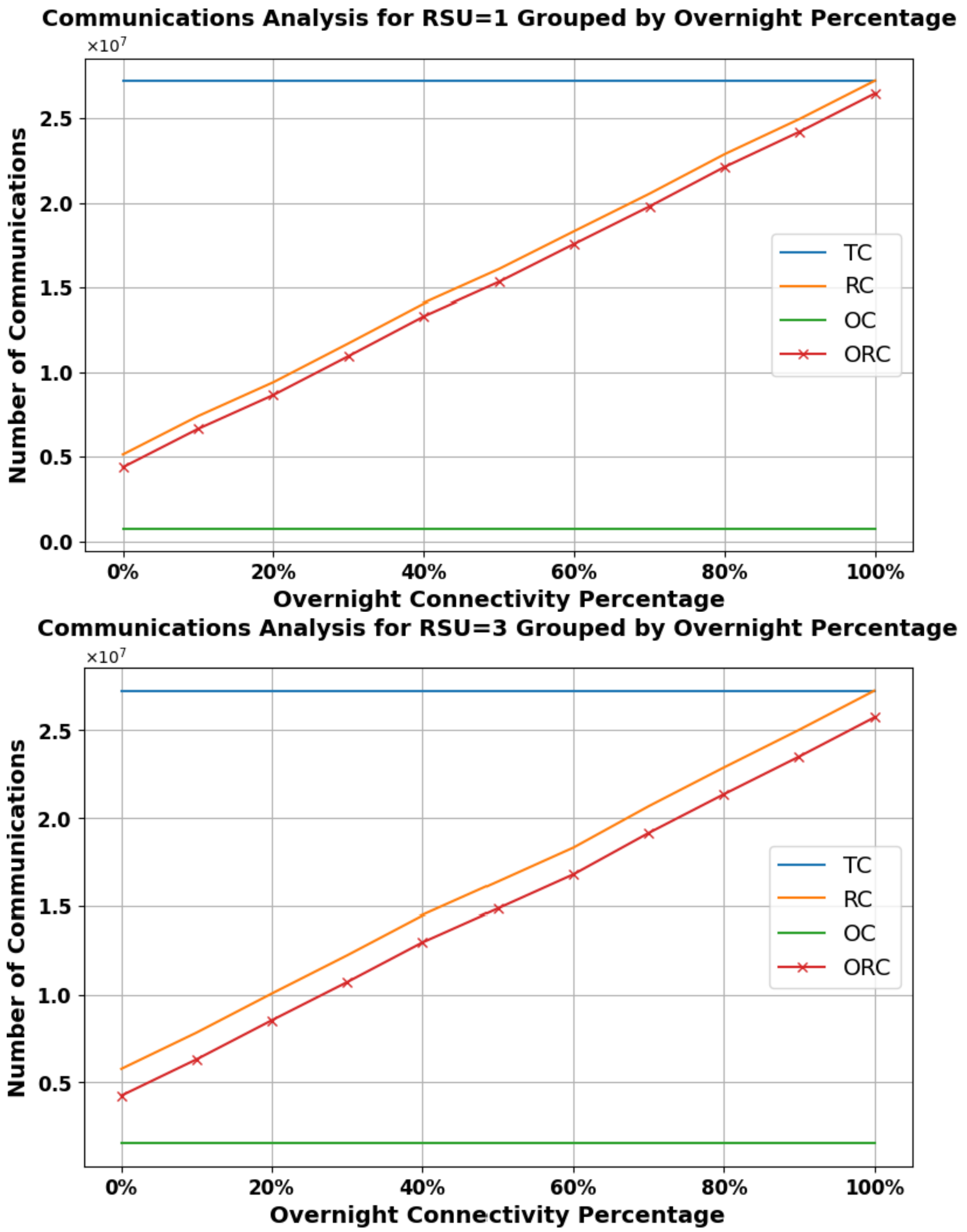


Figure 5.19: Analysis of Communication Types over Overnight Percentage in High RSU Range = 900 m for 1 RSU (**Left**) and 3 RSUs (**Right**).

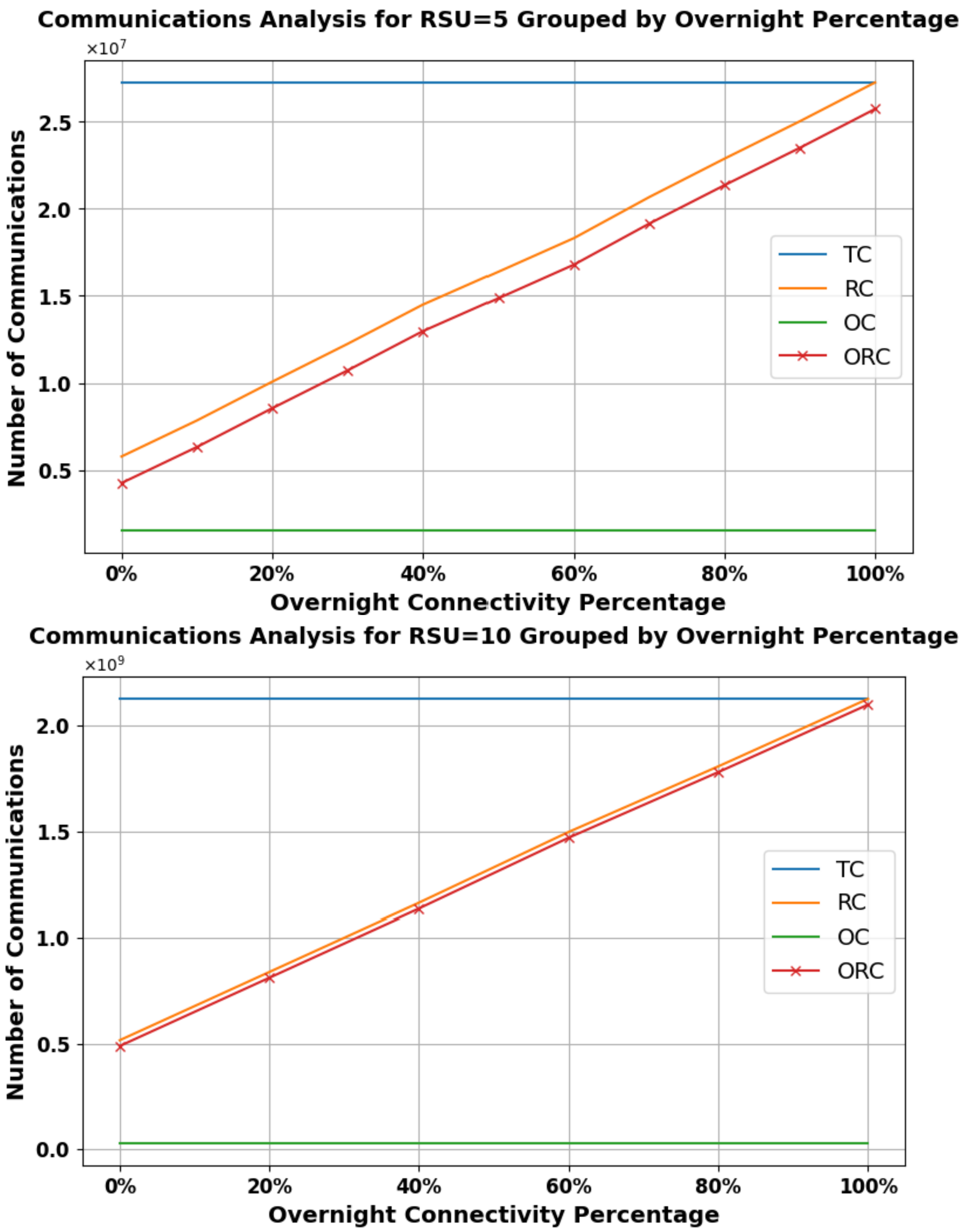


Figure 5.20: Analysis of Communication Types over Overnight Percentage in Low RSU Range = 300 m for 5 RSUs (**Left**) and 10 RSUs (**Right**).

This research measures connectivity on a scale from complete absence (0) to full coverage (100), revealing a direct relationship between the degree of connectivity and the quantity of reputable communications (RC). This trend suggests that, as vehicles gain better internet access overnight, they are more capable of updating their reputation metrics, showcasing the Pre-Signature scheme's potential in enhancing vehicular communication.

Notably, the graph sheds light on ORC, signifying that, even without RSU range, vehicles can still engage in trustworthy exchanges by leveraging pre-signed data, ensuring secure and dependable communication in areas with limited connectivity.

Observe that all graphs in Figures 5.19 and 5.20 are approximately linear. Having a large proportion of vehicles update their reputation overnight is one of the most effective ways to boost the quality of the proposed approach.

5.8.3 Results Synthesis: Pre-Signature Scheme in Rural Vehicular Communication Areas

The study on vehicular communication systems in rural settings places significant emphasis on the effectiveness of the *Pre-Signature* scheme, particularly in enhancing reputable communications in environments with sparse or non-existent RSU support. This scheme emerges as a pivotal solution for maintaining reliable and secure vehicular communication channels, especially in offline scenarios prevalent in rural areas.

The experiments show the effectiveness of the proposed scheme with different parameters and in different ways. In particular, the extent to which reputation disseminates over a 24-hour period and its impact on the number and proportion of reputable communications has been demonstrated.

Then, an investigation of how the adoption of RSU units affects the approach's usefulness is conducted, which shows that, in rural environments, increasing RSUs typically has a positive effect. Finally, the impact of drivers obtaining a Pre-Signature before entering the road is quantified, showing that this is an extremely powerful way to boost the effectiveness of the proposed approach.

A noteworthy aspect of the *Pre-Signature* scheme is its ability to uphold the integrity and trustworthiness of communications, regardless of RSU density. It ensures a consistent level of reputable communications, both online and offline. This is particularly vital in situations where vehicles operate outside the RSU range or in locations completely devoid of RSU presence. The study's findings highlight the Pre-Signature scheme as a key enabler for robust and dependable communication in rural vehicular networks.

5.9 Conclusion

This chapter has discussed into applying an innovative *Pre-Signature* scheme for V2V communications. Recommendations for changing standards, formats, and specifications are provided to ensure that the proposed approach is usable in the real-world. The approach is particularly suitable for rural landscapes where RSU availability is often limited or irregular. Through detailed simulations that closely emulate real-world rural scenarios, the study has provided an in-depth evaluation of this scheme efficiency under the typical infrastructural constraints of rural settings. This analysis not only highlights the key findings of the proposed Pre-Signature scheme but also sets the foundation for the next chapter, which delves deeper into using the Pre-Signature scheme to address conflicting messages during emergencies and attacks in rural areas.

Chapter 6

Reputation-Based Decision Accuracy in V2V Communication with Limited Infrastructure

The chapter investigates the deployment and effectiveness of the Pre-Signature scheme proposed in the previous chapter. It utilises it to improve decision-making in rural areas between vehicles during emergencies and attacks. The study compares the proposed system's efficiency against the existing certification system under varying accident conditions by implementing simulation-based experiments.

6.1 Introduction

As stated in the previous chapters, Vehicle-to-Vehicle (V2V) networking allows for safer, more secure and more efficient transportation by enabling vehicles to communicate and share messages to alert each other of incidents. However, there is a risk that malicious vehicles may insert fake messages, e.g., report a non-existent accident. Honest vehicles can dispute these fake messages, but similarly, malicious vehicles can dispute accurate reports. As a result, deciding which message is correct is challenging when receiving contradicting messages from multiple nearby vehicles. Existing standards supply the vehicles with (pseudonymous) certificates to meet the security and privacy requirements. If a vehicle is caught inserting fake messages, then its certificate can be revoked via a Certification Revocation List (CRL). In areas with limited connectivity (remote or rural areas), these CRLs may be out-of-date, and it may be difficult to establish the ground truth behind conflicting messages.

Reputation can help a vehicle make better decisions when confronted with conflicting messages where neither vehicle has revoked certificates. By adopting the *Pre-Signature*, reputation is available, even in the most challenging and infrastructure-limited area. This chapter provides the mechanisms to use reputation in areas with low/no connectivity, whilst allowing for pseudonymous certificates to verify message authenticity without breaking privacy. The approach is integrated into the existing SCMS standard.

The simulations evaluate the security performance of the proposed mechanism, with offline available reputation, against plain SCMS certificate management that rely solely on CRL to block malicious vehicles. The proposed scheme improves accuracy in decision-making with conflicting information by 36% in *Accidents* and 44.4% in *No-Accident* situations.

6.2 System Model

The system model first analyses vehicle behaviour in emergencies to present the threat scenario posed by the malicious behaviour in Section 6.2.1. This analysis sets the scene for the description of the proposed model in Section 6.2.2, which includes the decision-making process that forms the foundation of the work. Following this, explanations of reputation distribution and the system procedures are covered in Sections 6.2.3 and 6.2.4.

6.2.1 Operational Behaviour of Vehicles

Under standard V2V networking conditions, the majority of participating vehicles usually follow protocols and reliably report truthful information, and accurate road conditions resulting in maintained system integrity, safety, and trust. These vehicles are referred to as *honest* vehicles. However, a subset may have a tendency to send false information to disrupt communication or manipulate other vehicles intentionally, affecting the network trust system and potentially causing unsafe decisions. Such vehicles are classified as *malicious*.

Although the majority of vehicles may not be able to distinguish between honest and malicious activities, the attacker can communicate with each other through back channels with endless bandwidth, in addition to knowing which other vehicles are malicious, and cooperating with other malicious vehicles (e.g., by forwarding a falsified to mislead the recipient). This means that a message would be false if it is transmitted by even one malicious vehicle and it will differ from the correct message sent from the source vehicle.

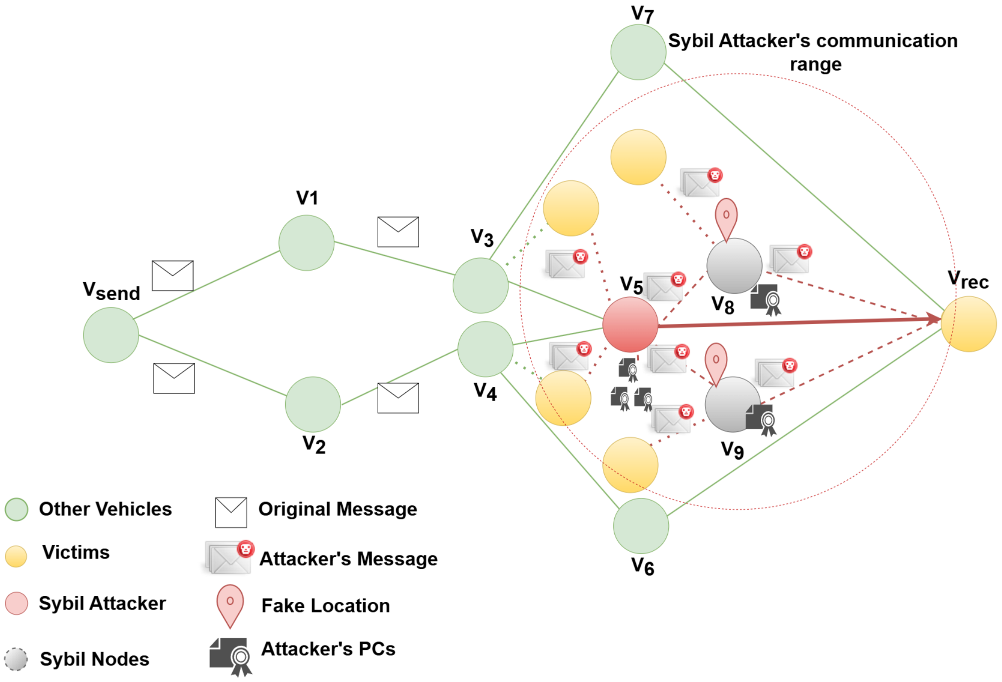


Figure 6.1: Illustration of Sybil Attack Threat Scenario.

As a high-risk example of malicious behaviour, the study considers an attack that is particularly powerful in a pseudonymous environment known as the *Sybil* attack, which creates multiple fake pseudonyms that could mislead the system into trusting fake nodes, hence controlling several false identities and amplifying the overall threat in V2V communication.

Figure 6.1 depicts the communication behaviour between different vehicles highlighting the misbehaviour activity of the Sybil attack. Let V_{send} denote the source vehicle that creates an emergency message (DENM) to alert other vehicles in the same area. The green nodes (V_1, V_2, V_3, V_4, etc.) represent honest vehicles that are behaving correctly forwarding or receiving messages as part of the system. V_1 and V_2 received the correct message from V_{send} and then forward it to V_3 and V_4. At this time, the red node V_5 represents the adversary (Sybil attack), who has actively created fake pseudonymous V_8 and V_9 (gray nodes) that are involved in malicious activities.

To illustrate, the incorrect attack messages that appear to originate from V_8 and V_9, as shown in Figure 6.1, are sent by V_5. V_5 achieves this deception by masking their true identity and using a falsified location and distinct pseudonyms associated with V_8 and V_9.

The lines connecting vehicles show the communication paths between them. The red dotted circle represents the Sybil attack range and the dotted solid lines represent the fake nodes communication, while the green lines represent communication from honest vehicles. As a result, victim vehicles (yellow nodes) within the adversary communication range, as well as the receiving vehicle V_{rec}, are affected by conflicting messages: False data from the Sybil nodes and potentially correct data from honest vehicles (green nodes).

The goal of the Sybil attack is to mislead recipients into believing the messages are from different vehicles. The attacker mainly relies on controlling Sybil nodes to broadcast false information, such as incorrect accident reports, leading to disrupted communication and incorrect decision-making by the affected vehicles. Thus, the attacker undermines the reliability of the sender's information and potentially bypasses verification protocols. Such actions manipulate communication and confuse the network, presenting security risks.

This study classified vehicle behaviour into two categories: *honest* and *malicious*. Honest vehicles behave normally and forward messages without any changes. On the other hand, malicious vehicles send false messages and mislead other vehicles to disrupt communication. Assuming that malicious vehicles work together and know the correct message that vehicle V_{send} is transmitting. They cannot change their or other vehicles' IDs, and the forwarding path list as signatures protected them.

Consequently, the attacker is limited to one of three malicious actions:

1. Disregarding the correct message.
2. Forwarding the incorrect message.
3. Crafting a counterfeit message.

While attackers might try to impersonate other vehicles, alter transmitted messages, or fake reputation values, the security properties of the model limit such abilities. For example, impersonation is not possible since pseudonym certificates bind each identity to a valid credential. Secure message signatures ensure message integrity; hence, any alteration of messages by unauthorised parties can be detected. The Pre-Signature mechanism considered in this study also protects the reputation system from attackers creating fake RVs. Thus, while attackers may have specific goals to compromise the system, these natural barriers and safeguards substantially limit what they can realistically achieve. However, the malicious sender can generates two types of reports: False negative and false positive reports.

The study focuses on the decisions made by a receiving vehicle V_{rec}, as it receives different copies of the DENM message. Theses DENM messages include an *Action-ID* in their structure. As referenced in the ETSI EN 302 637-3 V1.2.1 standards European Telecommunication Standard Institute ETSI72 (2019), the *Action-ID* acts as a unique identifier that specifies the type of action connected to an incident, like initiating, updating, or cancelling a report. In the proposed system, each incident reported is associated with an *Incident-ID* , denoted as I_{inc} which aligns with the *Action-ID* to emphasize its role in uniquely identifying and managing incident-related information. I_{inc} helps in grouping all relevant messages for consistent tracking and assessment.

The analyses include two situations: incident and no-incident events:

- Incident Situation

  In the incident situation, a false negative report is generated when the attack manipulates the emergency messages (DENM) to falsely transmit false information stating that there is no accident, resulting in undetected incidents and collisions with other vehicles. This situation starts with the honest vehicles reporting an incident with the associated I_{inc}, later the malicious vehicles may send messages to relay misleading information to the network in the form of honest reports using the same I_{inc}. In this case, the attacker aims to weaken the network's credibility by broadcasting conflicting information, which caused uncertainty and also possibly delaying responses to the actual incident.

- No-Incident Situation

  In this situation, a false positive report is generated when the attack sends fake emergency messages to falsely indicate an accident has happened, which triggers an unnecessary emergency response. Such messages can create confusion, delay critical responses, and exacerbate the consequences of real accidents. In this case, malicious vehicles start the scenario by creating and broadcasting false accident messages with an I_{inc} indicating there is an accident. As these false messages propagate, honest vehicles passing the location will report the correct status using the same I_{inc}, sending accurate information that contradicts the malicious reports. The attacker's goal in this situation is to manipulate traffic flow or exploit the system for personal gain, such as reducing congestion on their route.

A confusion matrix is utilised to visualize the performance of a classification model (Townsend, 1971). The matrix is used to assess system accuracy, in both incident and non-incident situations highlighting the impact of malicious behaviour on decision-making. In real incident cases, correct incident reports (true positives) can be overshadowed by false negatives due to malicious activities. In non-incident cases, false incident reports from malicious vehicles can lead to false positives, where vehicles unnecessarily alter routes, while honest vehicles help reduce confusion by sending correct messages (true negative).

	Predicted Positive	**Predicted Negative**
Actual Positive	True Positive (TP)	False Negative (FN)
Actual Negative	False Positive (FP)	True Negative (TN)

In the context of the study's focus, the classifications will be as follows:

- **True Positive (TP)**: Correctly identifying an actual accident.
- **True Negative (TN)**: Correctly identifying there is no accident.
- **False Positive (FP)**: Falsely indicating an accident has occurred.
- **False Negative (FN)**: Falsely stating there is no accident when one has occurred.

6.2.2 Proposed System

In V2V, every vehicle is assigned an authorised unique identification number ID through the Certification Authority (CA) in the SCMS. These IDs

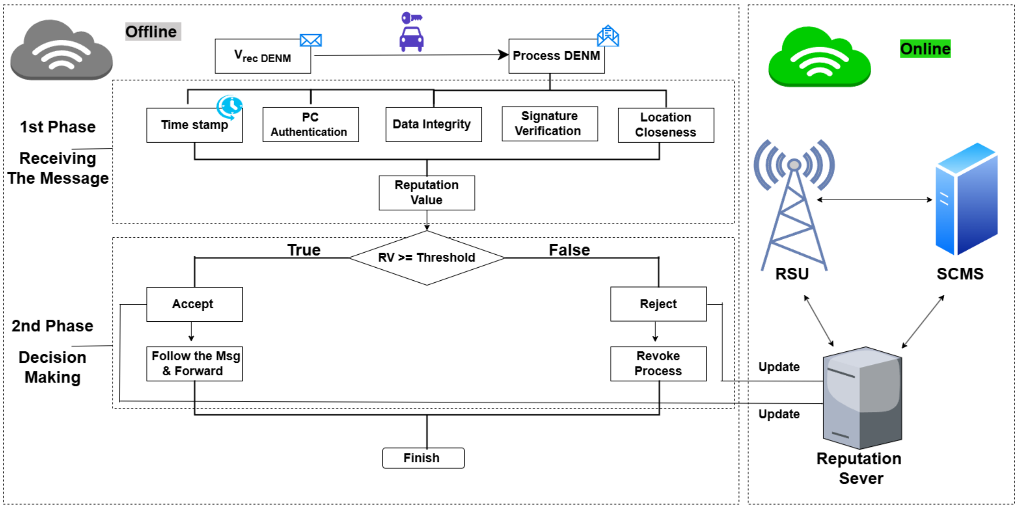


Figure 6.2: Phased Approach to Message Verification and Decision Making.

are already registered in the CA to prevent vehicles from faking their identity. In the proposed system, each message is associated with the Reputation Value (RV), which reflects the sender's historical trustworthiness. The Reputation Server (RS) updates the RV dynamically based on feedback from other vehicles. The system works as follows: Each day, vehicles should request a fresh pre-signature of their latest RV. Every time they switch pseudonyms, the vehicle computes a new completed signature. It is assumed that the sending vehicle V_{send}, which witnessed an accident, is an honest node, and most vehicles are legitimate nodes and CA-authorised.

The system model shown in Figure 6.2 represents the proposed approach that integrates reputation into the traditional certificate-based systems. In this approach, vehicles follow two verification processes: Certificate and Reputation to determine the authentication and the trustworthiness of a received message; improving security in the face of attacks (e.g.,Sybil attacks) and unreliable certificates.

The receiving vehicles (V_{rec}) verify the PC and RV signatures and check the sender's reputation score (V_{send}) before accepting and acting on a message. The reputation system enables vehicles to verify a message's source ad hoc without verifying via RSU or other infrastructure. Hence, a receiving vehicle can make a more accurate decision about whether to accept a received message and whether to forward or reject it. In the proposed system, upon receiving the DENM message, the verification processes should be executed in two phases, as described below:

Phase One: Receiving the DENM Message

1. **Certificate Verification:** First, upon receiving the messages, a V_{rec} verifies V_{send}'s PC against the CA signature on the certificate by using the CA's public key. This step ensures that the certificate is valid and that V_{send}'s public key is trustworthy.

2. **Verification of Digital Signature:** Next, V_{rec} verifies the message signature using V_{send}'s public key as represented on the certificate; the fact that such a signature is verified confirms both that the message comes from V_{send} and it has not been tampered with while in transit.

3. **Timestamp Validation:** The message timestamp is then verified by V_{rec} to be within an acceptable time window. This helps in preventing replay attacks where an attacker might resend an old message to confuse the receiver.

4. **Location Checking:** The message also contains the geographic location of the V_{send}, obtained via GPS. The location will be important for V_{rec} in the context of reaching a decision such as whether they are approaching the accident site or not and hence whether the information is relevant or not.

Phase Two: Reputation-Based Decision Making

In this phase, V_{rec} must verify the validity of V_{send}'s RV and evaluate it before deciding whether to trust the message. V_{rec} performs a preliminary check to authenticate the reputation, ensuring it is legitimate and has not been tampered with. By validating the reputation before relying on it, the system mitigates the risk of using falsified or manipulated RV. This enhances trustworthiness and accuracy in the reputation-based decision-making process. The RV verification process includes the following cases:

- Case 1: The message is considered trustworthy, and V_{rec} accepts the message if V_{send}'s RV is above a certain threshold. In this case, V_{rec} follows the message (e.g., reroute if an accident is reported) and forward it to other vehicles.
- Case 2: The message is considered untrustworthy, and V_{rec} rejects the message if V_{send}'s RV is below the threshold. In this case the message will be ignored regardless of its certificate validity.

6.2.3 Distribution of Reputation Values

In V2V networks, disseminating and sharing reputation information among vehicles is valuable for establishing trust levels based on their observed behaviours. Usually, the values of reputation range between 0 and 1, where 0 means highly distrustful or malicious behaviour, and 1 represents highly trusted or honest behaviour. In real-world scenarios, the vehicles would more likely exhibit a wide variation in trustworthiness; most would fall around the middle, where only a few would show extreme behaviours, either very honest or highly malicious.

The proposed system employs a distribution approach that distributes RVs rather than assigning a single score, the approach can represent both typical and extreme vehicle behaviours, providing a more nuanced basis for trust assessments. In this approach, a minimum RV, a maximum RV, and a most likely RV where most vehicles are expected to fall are set. Consequently, most of the vehicles-those that constantly follow the established protocols-will cluster around this central ”likely” value with a high RV. Only a small fraction of vehicles will deviate significantly from this norm, showing noticeably higher or lower RVs.

Moreover, a threshold value, τ , is introduced to enhance the reliability of decision-making. Setting a threshold allows the system to filter out potentially unreliable vehicles effectively. This threshold is the minimum RV required for a vehicle to be trusted. Vehicles with RVs equal to or above τ are treated as reliable, while those falling below this threshold may be flagged for closer monitoring or limited trust in communication. If RV_i represents the reputation value of vehicle i and τ is the threshold, the system defines a binary trust decision, T_i, for each vehicle i as follows:

$$T_i = \begin{cases} 1 & \text{if } RV_i \geq \tau \\ 0 & \text{if } RV_i < \tau \end{cases}$$

Where:

- $T_i = 1$ indicates that vehicle i is considered **trustworthy** (i.e., it meets the minimum reputation requirement),
- $T_i = 0$ indicates that vehicle i is considered **untrustworthy** (i.e., it does not meet the minimum reputation requirement).

6.2.4 Reputation System Procedures

The proposed reputation system ensures that only vehicles with a trustworthy RV should have their messages accepted. For clarity and consistency in representing the system's components, we use the notations in Table 6.1. Each vehicle has a C_i, which is a set of pseudonym certificates c_{ij} per each vehicles, these C_i are signed by CA_{SK}. A random c_{ij} signs each message M. In the proposed system, the RV is also attached to each message and signed with $V_{send}SK$.

Table 6.1: System Notations and Definitions

Notation	**Description**
V_i	Vehicle i
C_i	Set of pseudonym certificates for vehicle V_i
c_{ij}	Pseudonym certificate j for vehicle V_i
M	Message
$\sigma_{ij}(M)$	Signature of message M using certificate c_{ij}
$\text{Sign}_{c_{ij}}(M)$	Signing function using certificate c_{ij}
$\text{Verify}_{c_{ij}}(M, \sigma_{ij}(M))$	Verification function for M and $\sigma_{ij}(M)$
V_{send}	Sending vehicle
V_{rec}	Receiving vehicle
$V_{send}SK$	V_{send} Private Key
CA_{SK}	Certificate Authority Private Key
(K_{CA}^{pub})	Certificate Authority public key
$(K_{V_{send}}^{pub})$	V_{send} public key
RV	Reputation Value
τ	Reputation threshold
I_{inc}	Incident ID
τI_{inc}	Incident threshold

The *Incident-ID* is assigned a threshold based on the RV of the reporting vehicle, denoted as τI_{inc}. This ensures that the first report establishes the baseline (τI_{inc}), which serves as a reference for comparing subsequent reports. To illustrate, when the first DENM is broadcast after an incident, the *Incident-ID* is established in the DENM to uniquely identify the event. Alongside this, the V_{send} RV is evaluated. This initial RV sets the starting

τI_{inc}, which represents the minimum RV required for subsequent reports to be considered credible. As more reports are received, each vehicle's RV is compared against the current τI_{inc}. If a new report comes from a vehicle with an RV higher than the existing threshold, the system updates the τI_{inc} to reflect this higher value. For example, for a DENM to be accepted: The V_{send} RV must exceed an initial threshold τ, set at 0.5. The τI_{inc} is dynamically updated when a new DENM with a higher RV is received, DENM with RV below the current τI_{inc} is ignored. Generally, for the DENM to be accepted, it must satisfy:

$$RV_{V_{\text{send}}} \geq \tau \quad \text{and} \quad RV_{V_{\text{send}}} \geq (\{\tau I_{\text{inc}}\})$$

This ensures that only messages from vehicles with the highest reliability influence the understanding of the incident, maintaining a system that adapts to the most credible sources available.

The τI_{inc} also decays over time, but the rate of decay depends on the type of incident, which determines how long the information remains relevant. For example, information about a road closure should decay at a much slower rate than data about traffic congestion, which has a much shorter lifespan.

The system's workflow is explained in Algorithm 1. This algorithm begins by verifying V_{send} c_{ij}, using the CA public key (K_{CA}^{pub}). This step checks the signature of the c_{ij} to ensure it was issued by the CA. Once the certificate is verified, the V_{send} public key $K_{V_{\text{send}}}^{pub}$ is retrieved from the c_{ij} to later verify the message signature $\sigma_{ij}(M)$.

Algorithm 1 DENM Verification for V_{send}

```
Require: $(K_{CA}^{pub})$,$(c_{ij})$, $(RV)$, $(\tau)$, $(M)$, $(I_{\text{inc}})$, $(\tau I_{\text{inc}})$
Ensure: Validity (true/false)
Step 1: Check message validity of $M$.
if $M$ is invalid then
    return False
end if
Step 2: Extract $K_{V_{\text{send}}}^{pub}$ and $\sigma_{CA}(c_{ij})$ from $c_{ij}$.
Step 3: Compute $H(K_{V_{\text{send}}}^{pub})$.
Step 4: Verify $\sigma_{CA}(c_{ij})$ using $K_{CA}^{pub}$. If invalid, return False.
Step 5: Extract $H'(K_{V_{\text{send}}}^{pub})$.
Step 6: Compare $H(K_{V_{\text{send}}}^{pub})$ with $H'(K_{V_{\text{send}}}^{pub})$.
if $H'(K_{V_{\text{send}}}^{pub}) \neq H(K_{V_{\text{send}}}^{pub})$ then
    return False
end if
Check if $RV_{V_{\text{send}}} \geq \tau$.
if $RV_{V_{\text{send}}} \geq \tau$ then
    if $RV_{V_{\text{send}}} > \tau I_{\text{inc}}$ then
        $\tau I_{\text{inc}} \leftarrow RV_{V_{\text{send}}}$
        Log update.
    end if
    Verify consistency: $M \leftrightarrow I_{\text{inc}}$.
    Apply decay: $\tau I_{\text{inc}}(t) = \tau I_{\text{inc}} \cdot e^{-\lambda t}$.
    Check propagation rules.
    Record metadata.
    return True
else
    Log rejection.
    Notify $V_{send}$ if applicable.
    return False
end if
```

The algorithm then compares the hash of the $K_{V_{\text{send}}}^{pub}$ with the decrypted signature from the CA, confirming the certificate's authenticity. The RS assigns RVs below τ simultaneously with the Misbehaviour Authority (MA) in SCMS revoking certificates. This alignment ensures consistency, preventing revoked vehicles from regaining trust through reputation, enhancing overall security. Typically, the CRL would also be checked to ensure the V_{send}'s certificate has not been revoked. In an offline scenario, however, this is ineffective as the CRL can only be updated in real-time with connectivity.

This limitation makes this verification step unreliable, as the vehicle certificates that have been revoked might still appear valid, posing a significant security risk. In order to overcome this problem, the algorithm includes RV verification and checking by setting a threshold; for example, 0.5. If the V_{send} RV is greater than or equal to the threshold, the message is accepted; otherwise, it is rejected. As such, vehicles with records of trusted behaviour are still accepted even when updates to CRL are not available.

6.3 Simulation Design

This section discusses a simulation scenario, focusing on rural areas with limited infrastructure. The proposed reputation-based communication scheme is evaluated by comparing it with existing SCMS communication. First, the simulation tools used in this study are introduced. Next, the core concept of simulation and the design of the main scenarios are analysed, followed by a detailed discussion of how to set up the experiments.

6.3.1 Simulation Tools Integration

This simulation takes advantage of Simulation of Urban Mobility (SUMO), Objective Modular Network Testbed in C++ (OMNeT++), and Vehicles in Network Simulation (Veins) to validate the proposed reputation system. The combined simulation platform, as depicted in Figure 6.3, provides a realistic modelling of vehicular movements, network communications, and the complex interaction of vehicles exchanging emergency messages within the effective range of the DSRC of (1000 metres). Veins 5.2 framework was tuned to implement V2V simulations, which were based on OMNeT++ 5.6.2 (network simulator) and SUMO 1.19.0 (road traffic simulator).

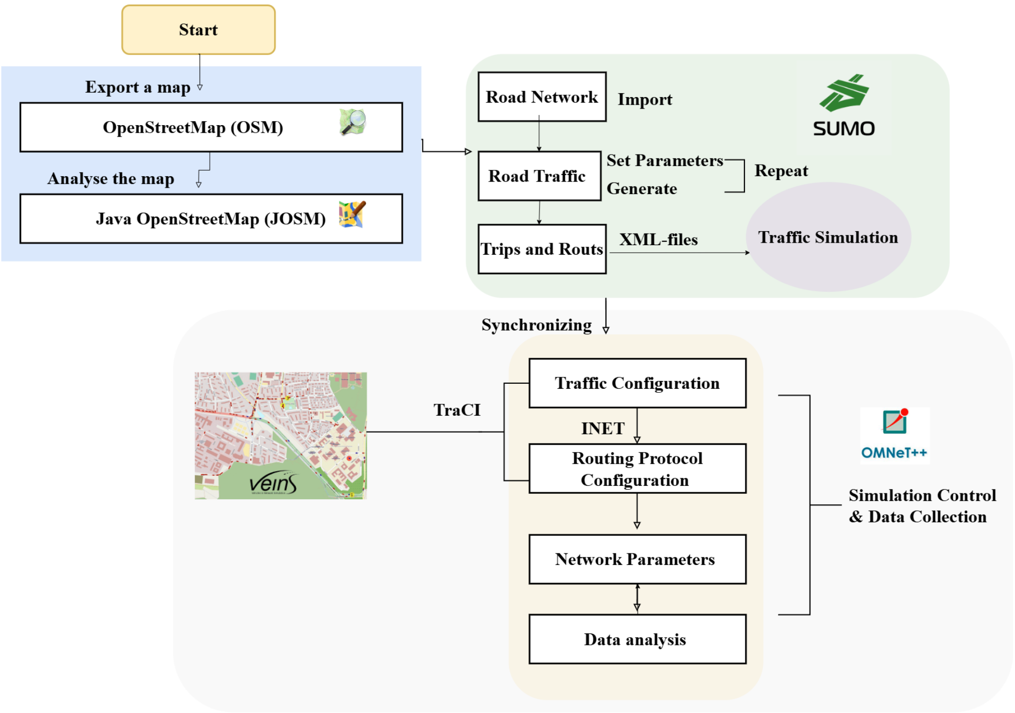


Figure 6.3: Integration of Simulation Tools.

The Trace Control Interface (*TraCI*) acted as an intermediary between OMNeT++ and SUMO, establishing TCP-based communication between the two simulators. The interaction between SUMO and OMNeT++ was done by API calls embedded in the Veins simulation. Such API calls, commonly referred to as commands, were available for both the *TraCIScenarioManager* and *TraCIMobility* modules of Veins. Each module allowed for direct interaction with the traffic simulation currently running in SUMO. A subset of these commands were utilised in the module's development. Furthermore, other commands that were not present in the TraCIScenarioManager or the TraCIMobility modules were implemented.

Triangle Distribution Of RVs

The triangular distribution is a widely used probability distribution whenever limited data is available, or an approximate estimation of values is needed (Jøsang, 2006).

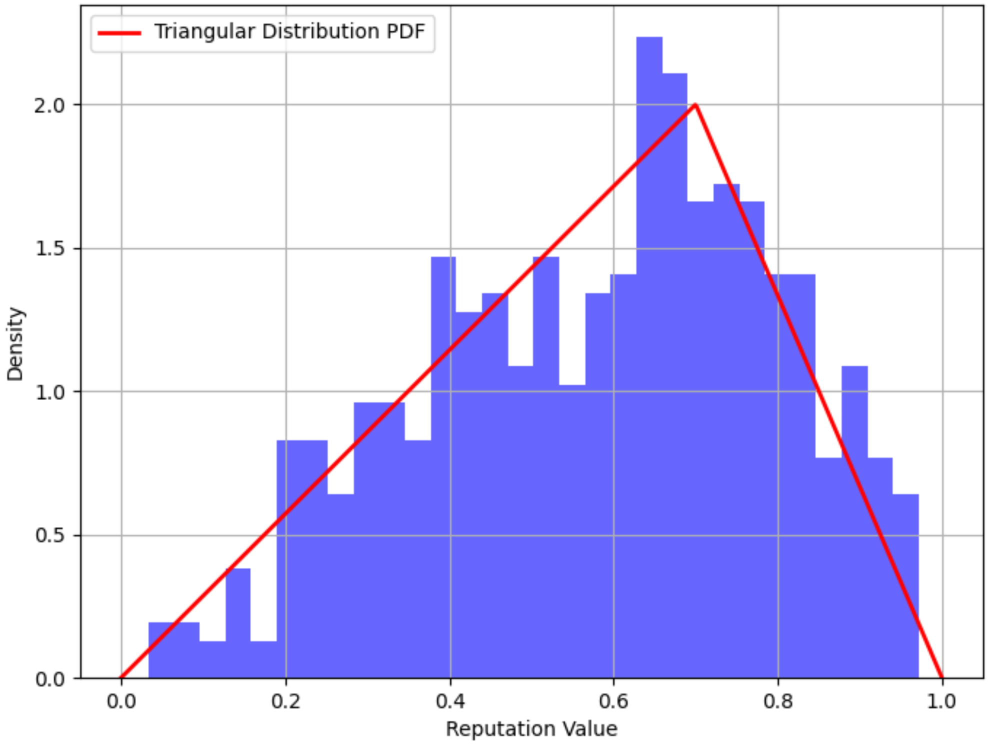


Figure 6.4: Triangle Distribution of the RVs.

This work, as shown in Figure 6.4, used the triangular distribution probability theory to distribute RVs among 500 vehicles. Using this theory, a situation is modelled in which most vehicles have average trustworthiness, while very few vehicles have extreme values (very low or very high). The triangular distribution is a continuous probability distribution. The lower limit a has been set to 0; the upper limit b has been set to 1, and the mode c, the most likely RV describes the reliability of the typical vehicle where $a \leq c \leq b$. Let for example $c = 0.7$. The Probability Density Function (PDF) of the triangular distribution is given by:

$$f(x) = \begin{cases} \frac{2(x-a)}{(b-a)(c-a)} & \text{for } a \leq x \leq c, \\ \frac{2(b-x)}{(b-a)(b-c)} & \text{for } c \leq x \leq b. \end{cases}$$

For the reputation distribution, the parameters are defined as follows:

- $a = 0$ (minimum RV),
- $b = 1$ (maximum RV),
- $c = 0.7$ (mode, or most likely RV).

6.3.2 Simulation Scenarios

The simulation focuses on V2V communication in the Peak District, a national park in central England, explained in (*Chapter* 2). The communications replicate real-world driving conditions under different scenario settings and over continuous simulation time frames. The simulation demonstrates the effectiveness of the *Pre-Signature* scheme since it enables vehicles to authenticate and validate messages for proper decision-making during such an emergency.

Two main scenarios were investigated, one with and one without an accident. For each scenario, the communication reliability was evaluated in two different simulations. The rationale for conducting simulations under both accident and non-accident situations is to assess the effectiveness of the proposed reputation system in mitigating the risks associated with the dissemination of false information. The accident scenarios test how vehicles respond to an actual hazard, while no-accident scenarios serve as a baseline to evaluate system performance in typical conditions without hazards.

Both scenarios are conducted using the map shown in Figure 6.5. The map is divided into four areas, each 1*1 km^2. The simulation measures the precision of the decision made by V_{rec} (node 7 in Figure 6.5) located at distance D from the sending vehicle.

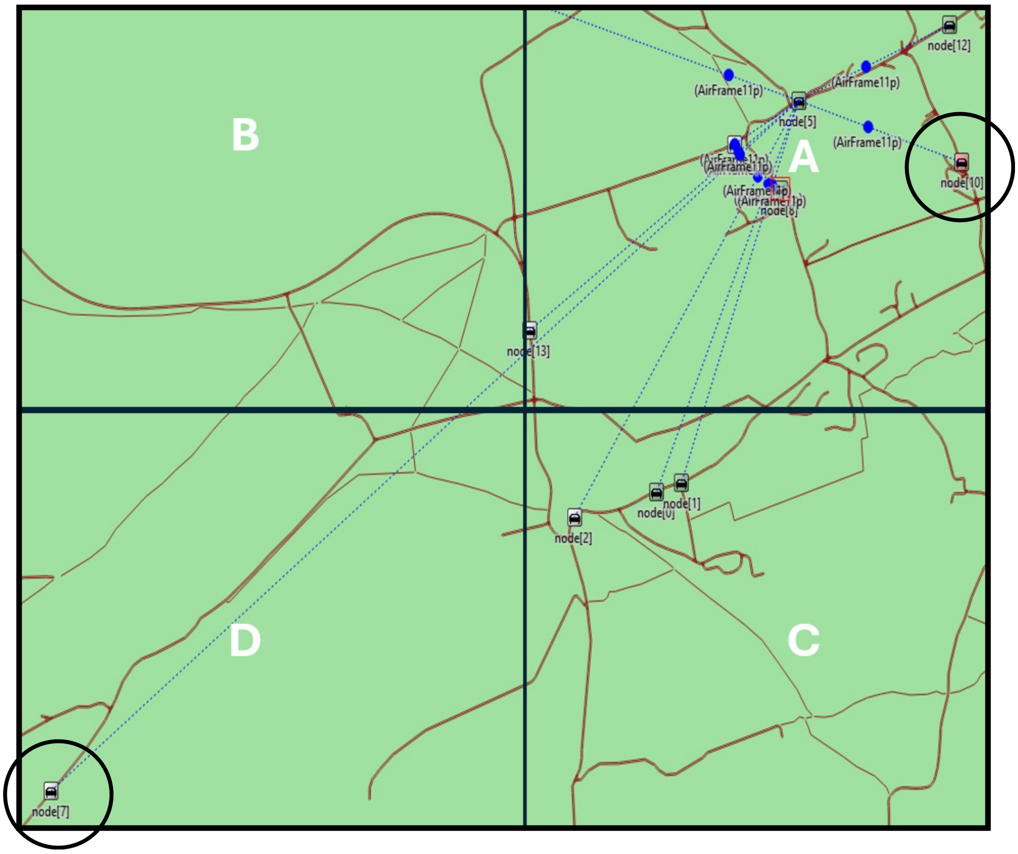


Figure 6.5: Target Area of Peak District Segment in OMNeT++.

The experiment includes a Sybil attack (node 10 in Figure 6.5) that manipulates communication accuracy by disseminating conflicting messages. Through simulation, vehicles exchange DENM messages for emergency notifications, which are represented as WAVE Short Message (WSM) in the Veins simulation. Similarly, DSRC is modelled using *IEEE 802.11p*, simulating realistic V2V interactions from Area A to Areas B, C, and D in different travelling directions, with a transmission range of R = 900-1000 metre. In both scenarios, the communication lines (blue dashed lines) show the WSM message exchanges. Table 6.2 shows the main scenarios.

Table 6.2: Summary of Examined Scenarios and Communications.

Scenario	**1st Simulation**	**2nd Simulation**
With Accident	Existing System (CRL)	Proposed System (CRL + RVs)
Without Accident	Existing System (CRL)	Proposed System (CRL+ RVs)

1. **First Scenario: Accident Event**

   In the first scenario, vehicles encounter an accident and alert each other using messages. In Quadrant A of Figure 6.5, where the accident occurs, vehicles near the accident, such as nodes (1),(5), and (12), broadcast the accident's occurrence, sharing correct information with nearby vehicles. V_{send} (node 5 in the map), which witnessed the accident, is considered a trustworthy node. However, the vehicles that depend on this information could be compromised. A Sybil attack (originating from node 10 on the map) generates multiple fake identities located in various places that transmit false information claiming that no incident occurred. This creates potential confusion for vehicles relying on the received data.

2. **Second Scenario: No Accident Event**

   In the second scenario, the map, communication protocols, timeline, and all other Sybil attack parameters remain the same. The variation presented here involves selecting a communication window in the period with no active accident to establish a clear baseline for testing in this scenario. In this scenario, node 10 initiates the scenario by generating fake emergency messages and then sends a false message with the same coordinates about an accident in quadrant A, trying to mislead the other vehicles in the surrounding area. After 20 seconds, an honest vehicle travels through the area, detecting no emergency, and generates a correct message that contradicts the malicious false alert, thus creating a true negative scenario.

3. **Comparative Dual-Simulation Approach**

   The simulation aims to follow the operation of existing certification systems such as SCMS,particularly the process of evaluating certificates against CRLs. In SCMS, the CRL plays a significant role in checking the validity of the exchange messages, typically checking if the attached certificate is listed in the CRL. If the certificate has to be found in the list, the message will be ignored; otherwise, the certificate is valid. However, this is not that effective in the theses scenarios because of the lack of connectivity in the disconnected areas. Instead, a reputation threshold similar to this concept is implemented. If a vehicle's RV is above a predefined threshold, its outgoing messages are considered valid and trusted. If the vehicle's RV falls below this threshold, the vehicle's messages are ignored.

   Two distinct simulation protocols are implemented in each scenario to assess their relative effectiveness. This approach allows for a direct comparison of how each simulation influences the scenario outcomes:

   (a) (1st Simulation:) The baseline communications uses CRLs.

   (b) (2nd Simulation:) The trust-based communication using RVs.

   In the *first simulation*, CRL-based communication serves as the baseline model. Where each vehicle is supplied with up to 100 PCs that are used for signing and verification processes. However, vehicles cannot reliably validate certificates without real-time updates. Offline communications delay CRL updates which means vehicles may continue to trust revoked certificates. The *second simulation* incorporates the communications using reputation by assigning random values to each vehicle using the triangular distribution probability theory (Jøsang, 2006) to distribute RVs among 500 vehicles.

6.3.3 Experimental Setup

This section discusses in detail the setting of the experimental environment and simulation parameters. The simulations have been carried out to validate the proposed scheme based on the protocols IEEE 802.11p/1609.4 (van Eenennaam et al., 2012). The simulation parameters have been chosen to reflect the characteristics typical of a rural area like the Peak District. Key parameters include the network size, mobility model communication standards, transmission range, and simulations time are specified in Table 6.3.

Table 6.3: Simulation Parameters.

Parameter	**Value**
Network size (km^2)	4*4
Mobility model	Peak Districts
Vehicle communication standard	(DSRC) IEEE 802.11 P
Transmission Range R(Mm)	250
Simulation Time (s)	12000
Number of vehicles per kilometre	10, 15, 20, 25, 30, 50
Data Transmission rate(Mbps)	27
Emergency packet size (bytes)	514
Emergency packet generation intervals (s)	0.05, 01, 05, 1
Minimum transmission frequency (Hz)	10
Required latency (ms)	< 100
Road side Unites (RSU)	0
Number of Accident	1
Accident Duration (s)	7600
Number of Sybil Attack	1
Vehicle Length	2.5
Road Type	Multiple-ways
Reputation Threshold	0.5

The scheme follows the following phases:

- **First Phase:** OSM map was imported into the SUMO platform in order to develop a realistic model of traffic simulation. Basic simulation parameters in SUMO, like the number of vehicles, the initial time of their trip, and the location of the vehicle, etc, were left unchanged to represent an actual communication for more realistic simulation scenarios.
- **Second Phase:** It integrated the SUMO output (XML files) with OMNeT++, using the Veins framework for simulating the behaviour of the vehicle under offline communication. In OMNeT++, the network topology (`.ned`) is designed for V2V communication, and the message file (`.msg`) is created, including all the information needed to design the DENM message.
- **Third Phase:** In this step, the Crypto++ library is integrated into the environment to implement cryptographic mechanisms, including certificate and key generation, signing, and verification.
- **Fourth Phase:** C++ source and header files were created to run the simulation and implement the designed algorithm.
- **Fifth Phase:** In this final phase, the parameters used in this study were specified, such as the simulation time and RV threshold in (`omnetpp.ini`) file, as shown in Table 6.3.

Based on the scenarios and simulation requirements described in the study design plan, as shown in Table 6.2, four different V2V communications were designed and explored:

1. Communication using Certificates during Accident (CCA).
2. Communication using Reputation during Accident (CRA).
3. Communication using Certificates with No Accident (CCNA).
4. Communication using Reputation with No Accident (CRNA).

In these communications, real-world traffic scenarios are utilised to explore different aspects of vehicle behaviours. Each communication starts with the initialisation stage, during which node parameters are set, certificates and RSA keys are generated, and counters for the metrics are initialised. For example, for each incoming WSM, the approach increments DENM counters, verifies message signatures, updates the route, and forwards messages if the sender's (RV $>= \tau$). The attacker nodes generate and schedule attack messages within the specified attack duration. The simulation logs the time, location, and range of each attack are recorded.

In addition, other functions are created to support the main procedures:

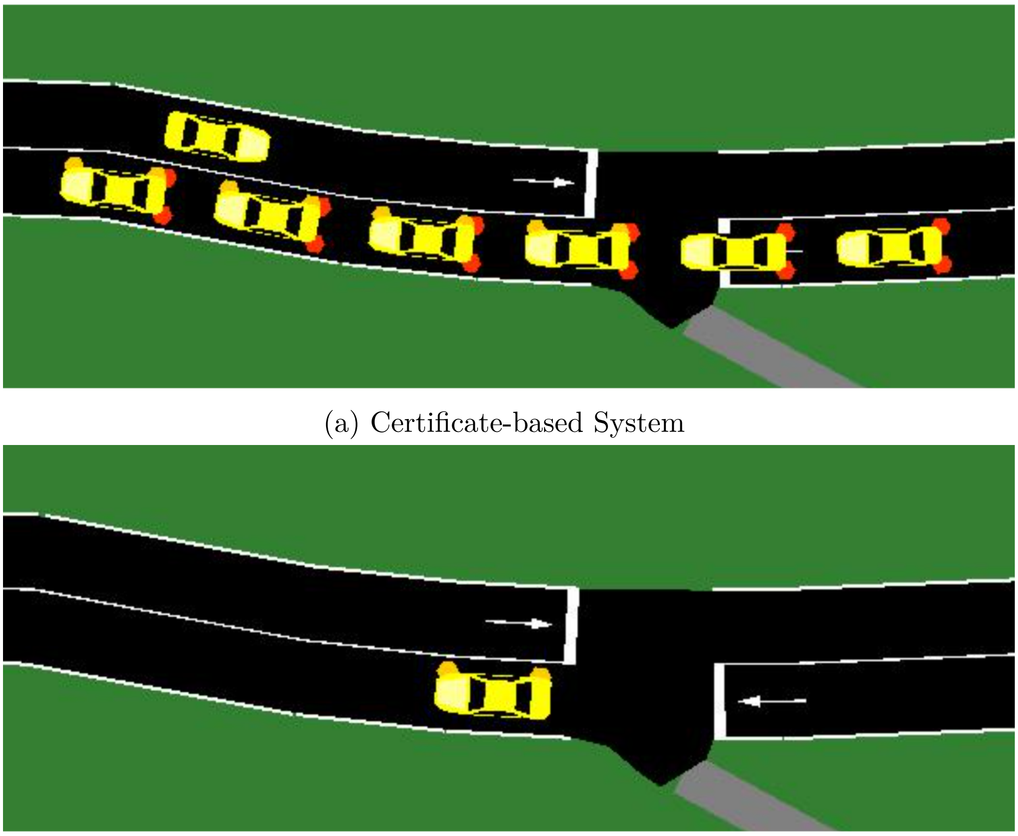
- Generating and storing certificates and RSA keys.
- Signing and verifying certificates and messages.
- Handling incoming messages.
- Handling the forward process and the route change.
- Managing the Sybil attack scenario.
- Recording scalar values for statistics.

For each scenario, six simulation runs were performed to ensure statistical reliability. Each run was initialised with a different random seed, which accounted for the variations in vehicle behaviour, network conditions, and other factors. The approach captured the randomness in vehicle mobility, message propagation, and network topology, that are critical elements affecting the results and analysis.

After running each experiment, all the statistics stored in vector and scalar files in OMNeT++ were analysed. The data was exported as csv files to store the relevant results and make them accessible for further analysis and visualization. This structured process allowed for easy comparison across the four experimental scenarios and provided a clear basis on which to conduct the statistical analysis. (*Appendix* B outlines the main steps of the simulation design and decision-making process).

6.4 Results : Performance Analysis and Evaluation

This section presents the overall results of the proposed vehicular communications simulation in a disconnected area. The aim was to compare the performance of the reputation approach with the existing standard SCMS in a rural environment with a sparse deployment of RSUs. The following analysis synthesizes data collected from the various simulation scenarios under different conditions. The findings provide insight into how the proposed reputation scheme improves decision accuracy under diverse conditions.



(a) Certificate-based System

(b) Reputation-based System

Figure 6.6: Screenshots comparing accident scenarios across communications using the (a) Certificate-based System and (b) Reputation-based System.

The screenshots in Figure 6.6 from the SUMO simulation GUI visually represent the communication scenarios in the two systems. These figures were taken early in the accident, (within 15 minutes). It is clear that adding a reputation system to the existing system minimizes the jamming of roads by limiting the spread of false messages, enabling vehicles to make informed decisions while re-routing effectively to minimize traffic congestion around accident sites.

6.4.1 Evaluating The Effectiveness of CRA and CRNA Over CCA and CCNA

This section analyses the two main scenarios: Accident and no accident in terms of True Positive (TP),True Negative (TN), False Positive (FP), and False Negative (FN) rates. As the study counts two types of vehicles: Honest and malicious performed by the Sybil attack, these rates are defined based on the decision accuracy made by the receiving vehicles as follows:

- (TP): Accepts a correct message from an honest vehicle.
- (TN): Rejects a false message from a malicious vehicle.
- (FP): Accepts a false message from a malicious vehicle.
- (FN): Rejects a correct message from an honest vehicle.

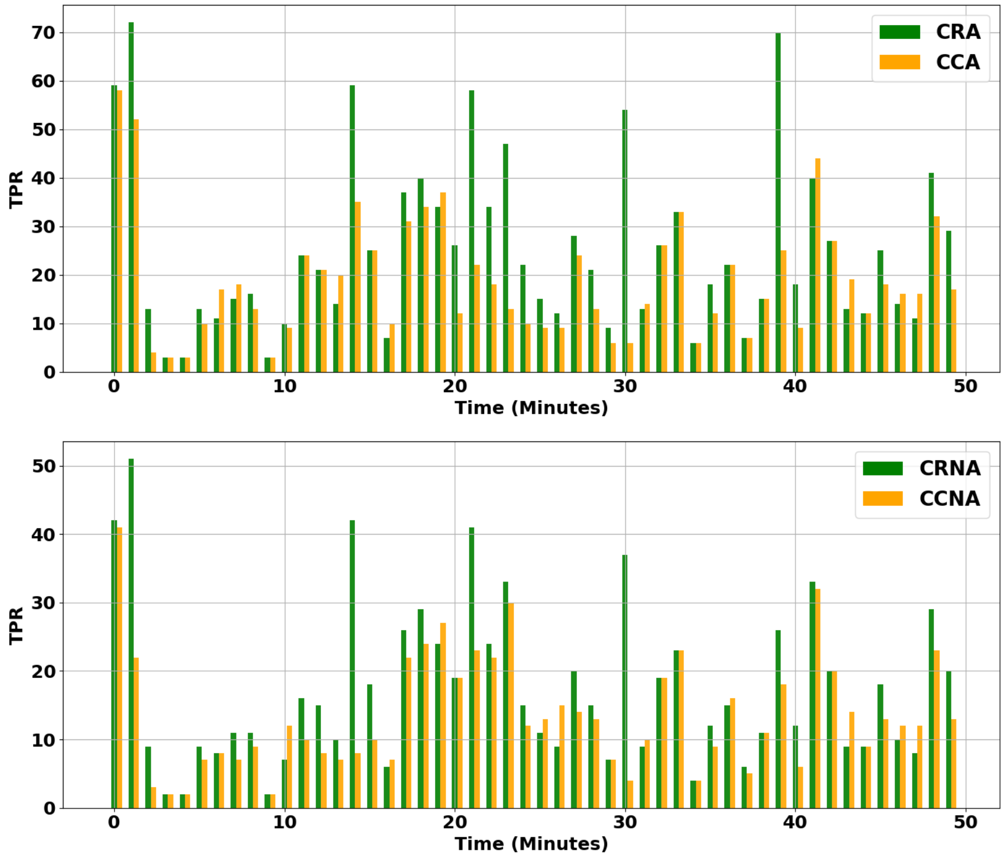


Figure 6.7: Comparison of **TP** Rates Across Vehicles in Accident Scenario **(Top)** and No Accident Scenario **(Bottom)**.

In Figure 6.7, CRA and CRNA show consistently higher rises in *(TP)* metrics compared to CCA and CCNA. This indicates that the V_{rec} using RV have better accuracy in accepting correct messages from honest sources indicating the exact accident condition.

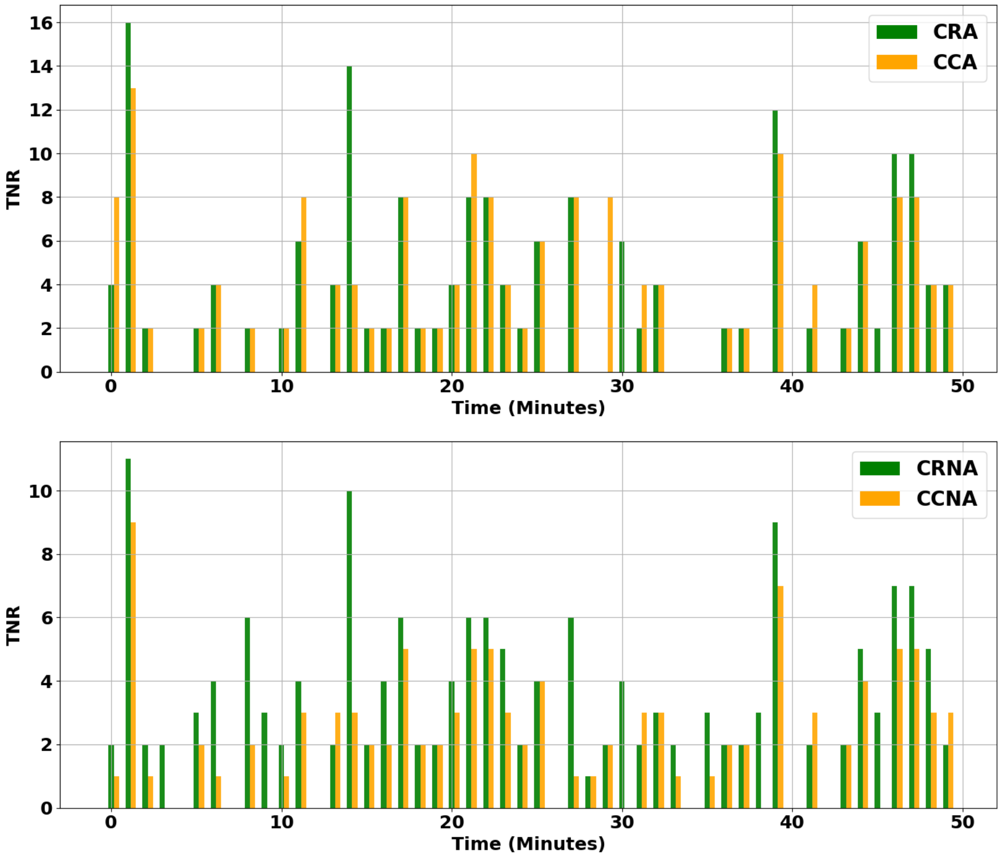


Figure 6.8: Comparison of **TN** Rates Across Vehicles in Accident Scenario **(Top)** and No Accident Scenario **(Bottom)**.

In Figure 6.8, it was observed that higher *(TN)* for CRA and CRNA compared to CCA and CCNA. This means that the V_{rec} using RV have better accuracy in rejecting the false messages from malicious sources indicating the wrong accident condition.

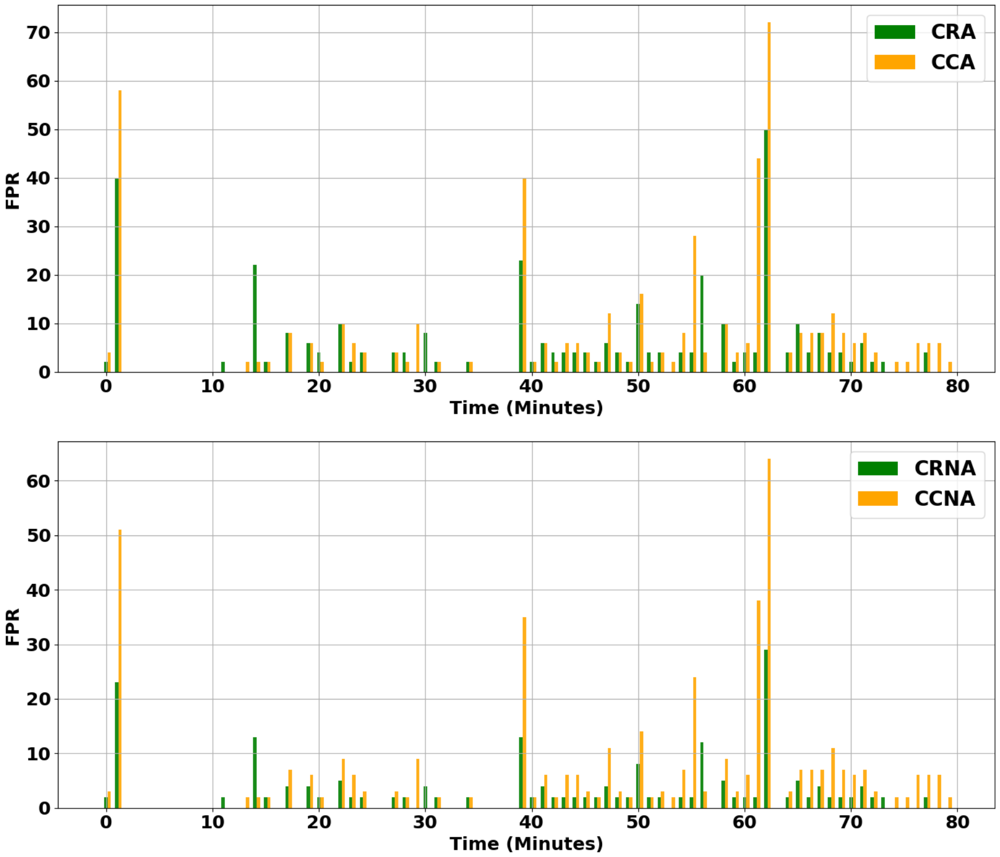


Figure 6.9: Comparison of **FP** Rates Across Vehicles in Accident Scenario **(Top)** and No Accident Scenario **(Bottom)**.

In contrast, Figures 6.9 and 6.10 show that for both conditions, the *(FP)* spikes are much higher in CCA and CCNA compared with the CRA and CRNA. This means that the existing communication using certificates might falsely accept incorrect messages from malicious sources, which further reduces its accuracy. Furthermore, Figure 6.10 presents more frequent and higher *(FN)* spikes with CCA and CRNA, especially during the early periods. This indicates that the existing communication misses more true messages than the reputation system, highlighting its reduced reliability.

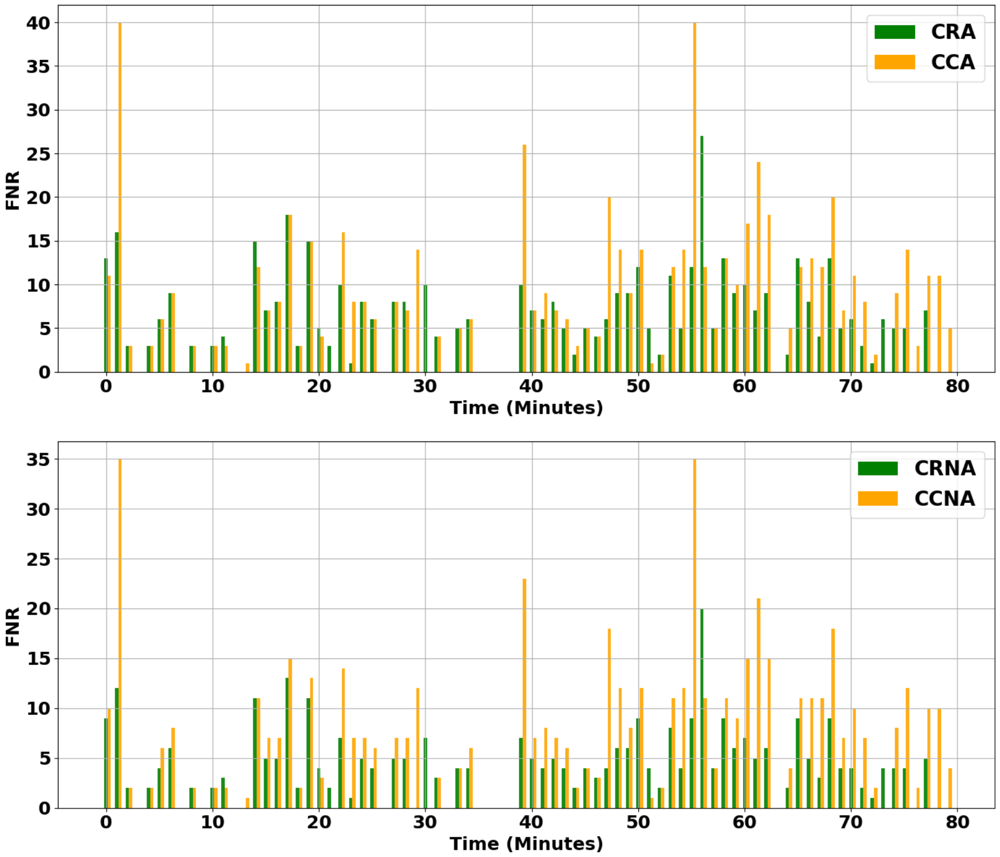


Figure 6.10: Comparison of **FN** Rates Across Vehicles in Accident Scenario **(Top)** and No Accident Scenario **(Bottom)**.

To further explain the results, the increased spikiness in the graphs is because of highly dynamic vehicle interactions and the great number of vehicles communicating within neighbourhoods, especially during the early simulation periods. In the accident scenario, this randomness amplifies fluctuations in message acceptance and rejection rates as trust and RVs are established. In addition, the complete lack of reputation-based filtering in the certificate-only systems allows the random acceptance of malicious messages to proceed unchecked, adding variability. This effect diminishes later in the simulation as the message patterns stabilize and interactions between vehicles decrease.

In general, the accident scenario (the top graphs) in Figures 6.7, 6.8, 6.9, and 6.10, shows higher communication compared with the No-accident scenario (the bottom graphs). This is because accidents involve a critical requirement for real-time information sharing in road safety. In such a scenario, vehicles are more likely to broadcast messages to forward the exact road condition, rerouting information, and warnings to surrounding nodes ensuring that informed decisions are made.

6.4.2 CRV and CPC Performance: Precision, Recall, and F-Score Analysis

The graphs in Figure 6.11, show Precision, Recall, and F-score over 200 minutes for the *communications based on Reputation (CRV)* and the *existing communications based on the certificates (CPC)* in both accident and no-accident conditions. Precision describes the ratio of correct messages correctly identified out of all the messages predicted as correct, while Recall gives the number of correct messages detected out of all actual correct messages, and the F-score balances both.

The precision and recall of CRA are significantly higher and more consistent, rarely dropping below 1.0. However, there is a noticeable decline in CCA, particularly at the 75- and 100-minute marks. This indicates that CRA tends to accept correct messages with fewer errors while missing fewer true messages, whereas the CCA incorrectly accepts many messages and misses a few more correct messages. Therefore, as reflected by the F-score, CRA has performed much better throughout.

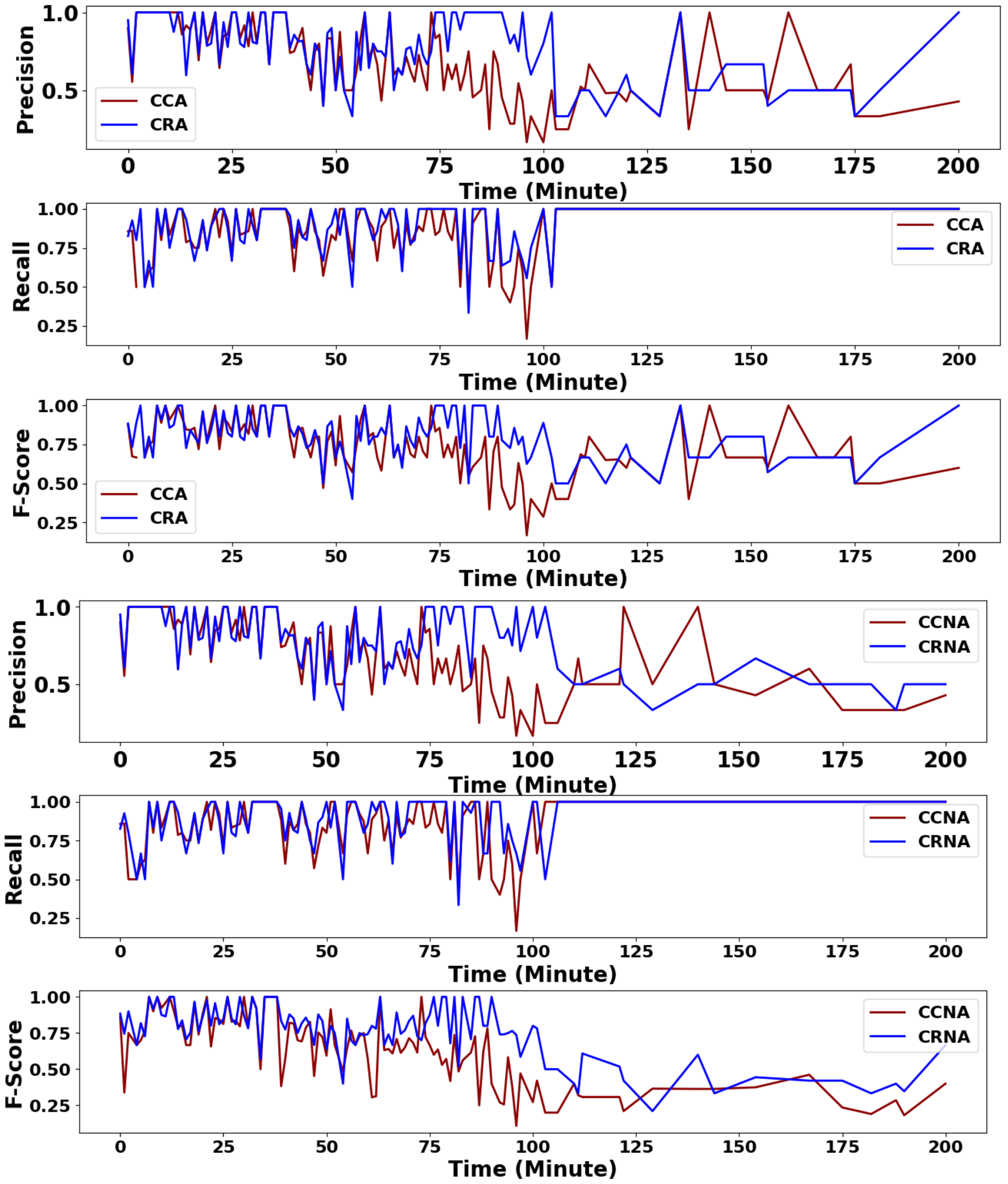


Figure 6.11: Performance of CCA, CRA (Top), CRNA, and CCNA (Bottom): Precision, Recall, and F-score.

There is more variation in the no-accident case for both, but again CRNA outperforms CCNA beyond the 100-minute input. Overall, CRV will prove more robust and exact, especially under accident conditions, since their Precision, Recall, and F-score are consistently higher compared to those of the CPC.

6.4.3 CRA and CRNA Impact on Decision Accuracy

High decision-making accuracy plays a significant role in message validation and maintaining efficiency in response, especially in disconnected areas. Higher accuracy would directly contribute to improved system performance, reducing FP and FN rates in handling messages. The accuracy of the decision-making in CRA and CRNA is calculated based on the correct identification of incidents using (TP), (TN), (FP), and (FN). This metric quantifies the improvement in accuracy provided by the *CRV* (Reputation Value) system over the *CPC* (Certificate baseline) system. Figure 6.12 shows the decision accuracy values in each communication.

1. For the Accident Scenario: The accuracy with reputation is 68%, and only 50% when using CRLs.
2. For the no accident scenario: The accuracy with reputation is 65%, and only 45% when using CRLs.

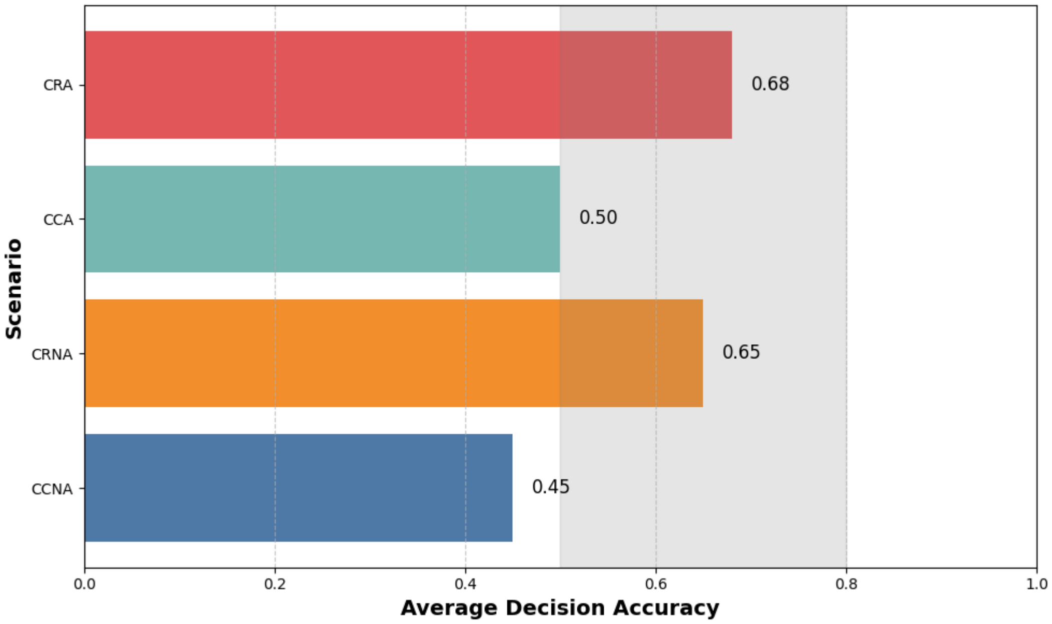


Figure 6.12: CRA and CRNA Impact on Decision Accuracy.

The proposed reputation approach improves accuracy by 36% in Accident scenarios and by 44.4% in No Accident scenarios over the existing communication system. The shaded area on the graph highlights the range of decision accuracy between 0.5 and 0.8, where the proposed reputation system consistently performs better. By filtering out untrusted messages, the proposed system ensures a more accurate and reliable communication environment in challenging communication with spare connectivity.

6.5 Conclusion

The study showed how reputation can be used to limit Sybil attacks activities and make more robust decisions when faced with conflicting messages. To measure effectiveness, four scenarios are simulated to compare the proposed reputation-based system performance against traditional methods that rely solely on certificate validation.

The results showed that adding reputation to the current certification system will consistently yield more accurate detection of correct messages with fewer false positives and missed detections. This underlines the relevance of reputation-based systems to provide trusted data transmission and it is resilient to fake reports, selective propagation of messages and Sybil attacks. The proposed reputation system enhances safety and enriches trust between vehicles in disconnected environments prone to malicious behaviour, and is compatible with existing pseudonymous protocols.

While this chapter used the proposed Pre-Signature scheme to address the issue of conflicting messages in rural vehicular networks, the next chapter will focus on the mechanisms for accurately reporting these conflicts, detailing how misbehaviour is identified and communicated to improve trust and accountability within the network.

Chapter 7

Distributed Reputation for Accurate Vehicle Misbehaviour Reporting (DRAMBR)

Following the previous chapter's analysis of conflicting messages arising from honest and malicious sources in rural areas, this chapter examines the accuracy of mechanisms for reporting misbehaviour in these contexts. It presents a novel approach for detecting and reporting malicious activities that compromise the integrity and reliability of V2V communication systems.

7.1 Introduction

In V2V communications, vehicles might misbehave by creating false or inconsistent information and sharing it with neighbouring vehicles, causing serious driving situations, (e.g. failing to report an observed accident or falsely reporting one when none exists). If other vehicles detect such misbehaviour, they can report it. However, false accusations constitute misbehaviour. In disconnected areas, the potential of misbehaviour increases, due to the scarcity of RSUs necessary for verifying V2V communications. Thus, detecting and reporting misbehaviour in such conditions is crucial and requires an accurate scheme that works offline without relying on an infrastructure. Vehicles need a reliable way to autonomously assess the trustworthiness of information based on factors like reputation scores.

A further difficulty is differentiating between genuine system errors, such as those resulting from imperfect GPS data, and intentional misbehaviour, a task that necessitates highly precise validation processes. Given the real-time requirements of vehicular networks, balancing data accuracy and computational efficiency poses a dilemma. In addition, the emphasis on privacy protection using certificates to maintain anonymity, complicates the process of misbehaviour detection. Existing standards for misbehaving detection and reporting rely on the Misbehaviour Authority (MA) in the SCMS (Brecht et al., 2018), as explained in (*Chapter* 3). In this system, if enough misbehaviour is reported for a certain vehicle, the vehicle certificates will be revoked and added to the Certification Revocation List (CRL). This will be updated and distributed to other vehicles in the environment. However, in disconnected areas, vehicles can face difficulties communicating with the SCMS in such challenging situations, leading to certificate issuance and renewal delays as outlined in the previous chapters.

This chapter proposes a novel mechanism, Distributed Reputation mechanism for Accurate Misbehaviour Reporting *(DRAMBR)*, offering a fully integrated reputation solution that utilises reputation to enhance the accuracy of the reporting system. DRAMBR becomes particularly relevant in contexts where direct authority oversight is limited, or when vehicles cannot operate in fully connected manners. DRAMBR improves the accuracy of vehicle misbehaviour reporting using two processes of assessment:

1. **Offline Misbehaviour Detection:** During offline communication, a vehicle detects misbehaviour, collects observations from neighbours, and generates a Misbehaviour Report (MR).

2. **Online RS Processing:** Upon reconnection, the MR is sent to the RS, which performs validation steps, aggregates data, and takes appropriate action on the reporter and target vehicles.

DRAMBR processes and evaluates MRs through a multi-stage aggregation process integrating advanced classification techniques such as DBSCAN, Isolation Forest, and GMM. The vehicle's communication is analysed under different conditions using SUMO. DRAMBR's accuracy performance is then evaluated using Random Forest and XGBoost, suggesting that it provides an accurate reputation management approach under challenging conditions. DRAMBR distinguishes between honest mistakes, intentional deception, and malicious reporting. The system's performance is evaluated, demonstrating its effectiveness in achieving a reporting accuracy of approximately 98%. The findings highlight the potential of reputation-based strategies to minimize misbehaviour and improve the reliability and security of V2V communications, particularly in rural areas ultimately contributing to safer and more reliable transportation systems.

7.2 DRAMBR System Model

DRAMBR represents a fully integrated reputation solution designed to manage the reporting process effectively under challenging conditions in V2V communication. The aim is to enhance the trustworthiness of V2V communications by monitoring vehicle platoon behaviour, detecting any misbehaviour, and reporting it back to a central Reputation Server (RS) that assigns and periodically updates their RVs to demonstrate their trustworthiness.

The system operates in two primary phases: Offline Evaluating (OE) and Online Reporting (OR): In the OE, vehicles assess each other's behaviour and store Misbehaviour Report (MR) locally without central connectivity, enabling continuous trust management. In the OR phase, upon reconnection to the Internet, the vehicles send the accumulated MRs to the RS. The RS aggregates, classifies, and analyses the MRs, reducing processing overhead.

The system can be implemented in both urban (*online*) and rural (*offline*) areas. In urban areas, it reduces computational complexity on the RS, by decentralizing the Reputation Values (RVs), thereby improving scalability and efficiency. In rural areas, vehicles benefit from sharing their RVs without relying on a central authority, ensuring continued reliability even in disconnected scenarios.

This section first outlines the main system assumptions. Next, it explains the vehicle behaviours highlighting the threat model relevant in this study. Following that, the DRAMBR framework is introduced. These explanations set the stage for discussing the main phases of DRAMBR.

7.2.1 DRAMBR Assumptions

To ensure realistic communication network, the study relies on assumptions about vehicle capabilities, behaviours and system conditions. These assumptions reflect practical and feasible conditions in real-world vehicular networks.

- Pseudonymity: Vehicles interact via pseudonyms and communicate over an anonymous network.
- Connectivity setup: In the OE phase, vehicles communicate out of range of network connectivity, hence, the periodic synchronization with the network to obtain the latest CRLs and RVs is limited.
- Reputation setup: Each vehicle is initialised with an RV. The RV will increase with positive behaviour and decrease with misbehaviour.
- Independent behaviour: Each vehicle can behave either honestly or dishonestly. A vehicle's behaviour is independent of others such that the actions of vehicle V_i do not influence the behaviour of vehicle V_j.
- Communication range: Vehicles communicate using Dedicated Short-Range Communication (DSRC) technology that has been developed specifically to provide reliable communication within a range of (1000 metre), ensuring only nearby vehicles can interact even without connectivity.
- OBUs detection: Each vehicle is equipped with On-Board Units (OBUs) that can detect any abnormal activity or irregular behaviour.
- Messages checking: Each vehicle has a mechanism to check its outgoing messages and detect any misbehaviour before they are transmitted.

- Limited misbehaviour reporting: Not all observed misbehaviour activities lead to the generation and transmission of MR. The decision about whether a vehicle generates an MR based on observed misbehaviour is specific to that vehicle's implementation.

7.2.2 Vehicle Behaviour in OE and OR

Vehicles can act very differently on a network depending on their intentions and strategy. While an honest vehicle always follows protocols and truthfully report, malicious ones may exhibit dynamic behaviour; for instance, by deliberately causing harm in the system, such as sending misleading information or behaving strategically honestly with the intent of gaining confidence to get undetected, their actions will be challenging to anticipate and control. Generally, trust and reputation-based systems are exposed to two main behaviours listed below:

- **Honest**:
  1- In V2V, create, broadcast, or forward correct messages M_{sgs} (OE Phase).
  2- In V2I, create and submit correct MRs(OR Phase).
- **Malicious**:
  1- In V2V, ignore the correct messages M_{sgs} or create and broadcast false M_{sgs} (OE Phase).
  2- In V2I, create and submit false MRs (OR Phase).

The system makes a distinction between intentional and unintentional misbehaviour, see Figure 7.1, with the latter encompassing all vehicle faults and error scenarios.

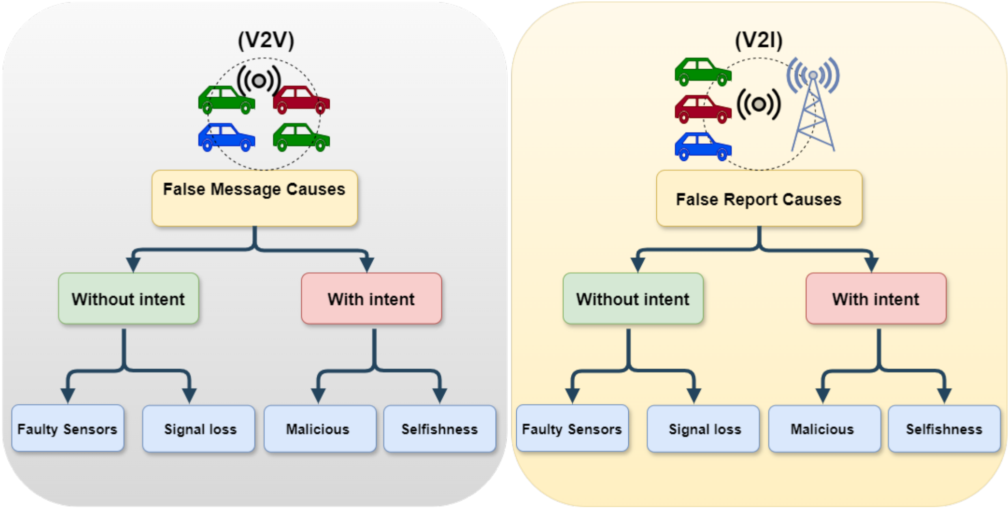


Figure 7.1: False M_{sg} / MR_f Causes.

While the system takes into account all these considerations, the primary focus is on the accuracy of the MR submission and the behaviour of the reporters. Specifically, analysing the causes of false MR (MR_f) and how the reporter's reliability impacts the overall trustworthiness of the system. A significant threat scenario arises by an *MR Attack* (MR_fReporter), when an attacker with a high RV manipulates the reporting system by not reporting misbehaviour and generates a MR_f for an honest vehicle, as illustrated in Figure 7.2.

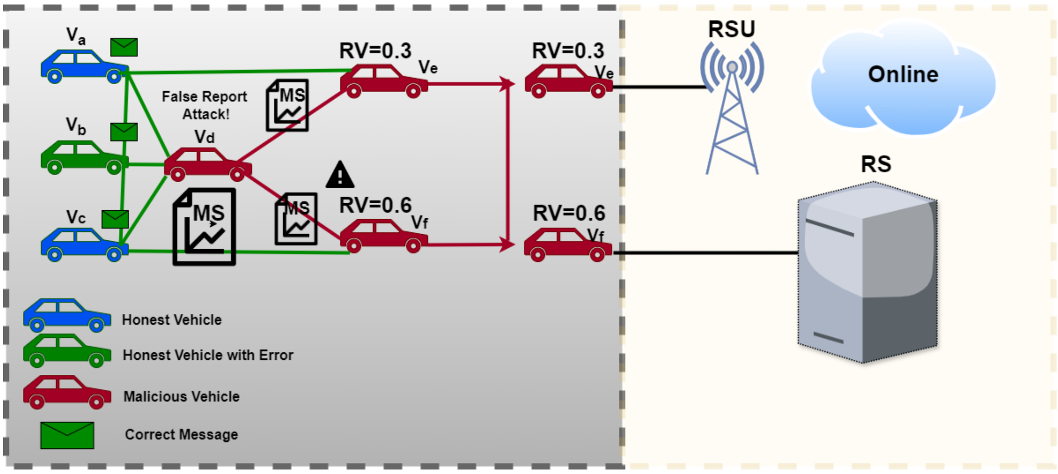


Figure 7.2: MR Attack.

This type of activity is similar to the badmouthing attack (Banković et al., 2011), which might result in assigning a high RV to a vehicle that deserves a lower one and vice versa. This tactic inflates the reputation of certain vehicles, making them seem more trustworthy while deflating the reputation of others and harming their credibility.

Algorithm 2 MR_{Attack}

```
Input: $V_j$, $S(V_j)$
Output: $MR_f$ or Null
if $S(V_j) \neq$ "misbehaving" then                ▷ Target is honest
    $MR_f \leftarrow$ GenerateMR($V_j$) + AttachCertificate($PC$)
    Send $MR_f$ to $RS$
else
    $MR_f \leftarrow$ Null                ▷ No MR sent for misbehaving vehicle
end if
```

Such rating manipulation distorts the accurate feedback, misleads other vehicles, and undermines trust in the platform's rating system. The MR_{Attack} algorithm shows the attack activity considered in this chapter. Assuming V_j is behaving honestly, the attacker targets V_j by generating a false misbehaviour report (MR_f). The (MR_f) is generated only if the status of target vehicle is not already flagged as misbehaving ($S(V_j) \neq$ misbehaving). However, if the target vehicle is already flagged as misbehaving, no MR is sent, and the attack halts. To mitigate such an attack, the proposed system follows a thorough process of comparison and aggregation, ensuring a more accurate evaluation as illustrated in the following sections.

7.2.3 DRAMBR Framework

DRAMBR framework is shown in Figure 7.3. As described in the proposed system within this thesis, the Reputation Server (RS) is linked to the Misbehaviour Authority (MA) in the SCMS.

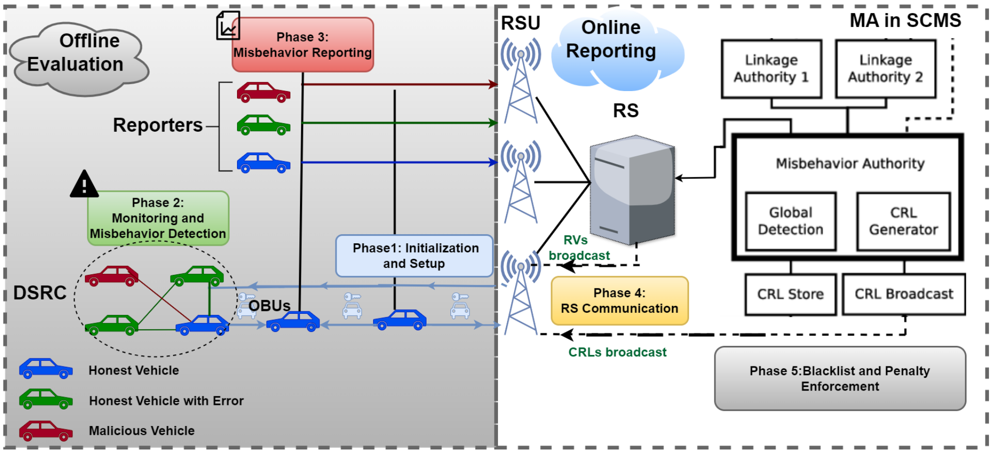


Figure 7.3: Proposed Misbehaviour Reporting System (DRAMBR).

During the reputation retrieval process, the RS will pre-sign the RV using the *Pre-Signature* scheme proposed in (*Chapter* 5). The RV is then sent to the requested vehicle to complete the signature and attach it with the PC to the message. All MRs are submitted to the RS, which checks and evaluates all the received MRs. A threshold for accepting the MR is set as τ_{Rep}.

The vehicle reporting the misbehaviour is denoted as (Rep_{Veh}) and the target vehicle as (Tar_{Veh}). The reputation system is designed to consider MRs if they meet τ_{Rep} and ignore any MR from Rep_{Veh} where $RV < \tau_{Rep}$.

The system's efficiency is highlighted by its ability to handle contradictions between the MRs accurately. If most MRs contradict a specific MR, indicating the same misbehaviour, the RS evaluates the context before classifying it as malicious, considering errors or potential attacks to ensure fair decisions and system reliability. To set the stage for the DRAMBR valuation process, the main entities involved, as outlined in Table 7.1.

Table 7.1: DRAMBR System Units.

Unit	Purpose	Connectivity
OBU	Detecting misbehaviour, generating MR, and interacting with other vehicles and the RS.	Online/Offline
RS	Aggregates MRs and adjusts the RVs.	Online
DSRC	Facilitates V2V and V2I communications.	Online/Offline
MA	Global misbehaviour detection, generating and broadcasting CRLs, and creates and stores the CRLs.	Online

7.2.4 Workflow and DRAMBR Phases

As shown in Figure 7.3, DRAMBR begins with the registration phase, the *initial phase*: In this phase, vehicle are connected to the infrastructure (RSU or RS) establish unique credentials and download the PCs as well as retrieve the RV. The overall process is divided into two broad stages that are: Offline Evaluation (OE) and Online Reporting (OR) each further divided into sub-phases to present an integrated security and trust management for V2V communication.

Process 1: Offline Evaluation (OE)

This phase occurs *offline*, where vehicles evaluate the accuracy of road status information within the offline network. Vehicles monitor each other's behaviour and trustworthiness in an ad hoc manner, without relying on trusted authorities to identify potential misbehaviour. Before discussing the main steps in the OE process, the critical events that trigger the local detection and evaluation mechanisms within the system will be explained.

The trigger event $O(M)$ for identifying misbehaviour occurs when the $Tar_{\text{Veh}}(V_j)$ transmits contradicts observable conditions, which is the basic event that drives the system responses. $O(M)$ could indicate misbehaviour in two possible activities:

- Failure Alert Transmission: When V_j detects an incident but does not transmit it, nearby observing vehicles (Rep_{Vehs}) may detect this omission through their OBUs or reports from other vehicles.
- False Alert Transmission: When V_j transmits an emergency when no accident or hazard exists, observing vehicles compare this false claim with their OBUs data and messages from others.

These misbehaviour activities are referred to as conflicting messages, where multiple messages provide inconsistent or contradictory information. While the previous chapter addressed the issue of receiving conflicting messages, this study focuses on accurately generating MRs based on observations in offline mode as part of its broader scope.

Table 7.2: Rep_{Veh} Observing Misbehaviour Action.

Notations	$Rep_{\textbf{Veh}}$ **Action**
O(R)	Observing misbehaviour and generating a MR.
O(NR)	Observing misbehaviour but not generating a MR.
O(NMR)	Not observing misbehaviour but generating a MR_f.
O(NNMR)	Neither observing nor generating.

Various possibilities exist for reporting abnormal behaviour under emergencies as stated in Table 7.2. Outlining these actions is essential to analyse and evaluate the vehicle behaviours in various scenarios involving emergency events. The table shows different possibilities that vehicles can take based on whether they observe a misbehaviour and whether they intend to

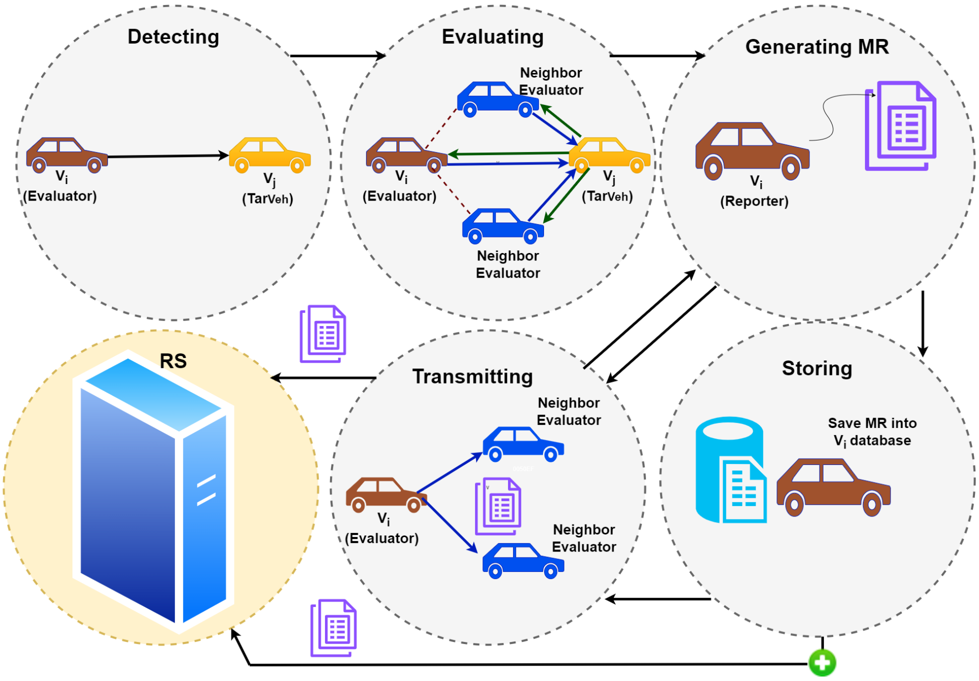


Figure 7.4: Local Misbehaviour Detection Mechanism (LMDM).

generate an accurate or false MR. *O(R), O(NR), O(NMR), and O(NNMR)* capture different aspects of reporting behaviour, including truthful, non-reporting, or malicious reporting. These action estimations become part of the system process to aid in decision-making, wherein the RS assesses incoming MRs and verifies them through RVs, cross-verification, and the likelihood of correct reporting behaviour.

The study proposes a multi-step process called Local Misbehaviour Detection Mechanism (LMDM) in order to cope with insider attackers, see Figure 7.4. LMDM represents the OE process operating at the local level to detect misbehaviours by analysing reports and interactions within a localised scope. It is a component of DRAMBR that detects misbehaviour locally by directly observing malicious activities (e.g., directly observing a situation incompatible with a received message) or indirectly by receiving conflicting messages, at least one of which must be false. The remainder of DRAMBR concerns storing, reporting, aggregating and integrating the observations. The detection criteria in this phase are as follows:

- Message Integrity: Ensure that received messages are not altered.
- Communication Frequency: Detect flooding attacks if a vehicle sends an excessive number of messages.
- Message Validity: Verify that the content of the message (e.g., location or speed) matches observed reality.

In this stage, preliminary misbehaviour reports are generated based on immediate surroundings (direct observation) or V2V communications (indirect observation). The LMDM outputs serve as inputs to the DRAMBR OR process. *LMDM* includes five main steps as explain below:

1. **Detection**: The OBUs of the evaluator (V_i) actively detect and identify irregularities and potential misbehaviour within the network.
2. **Evaluation:** V_i evaluates the misbehaviour to decide whether or not to generate an MR for the observed misbehaviour event. To confirm the misbehaviour through collective evaluation, V_i communicates with nearby vehicles if any are present. If no other vehicles are available in the area for verification, V_i proceeds to make an independent decision based on the available evidence. This approach has been discussed in (Lv et al., 2022), where vehicles collaborate to validate suspicious activities.
3. **Decision**: In this phase, V_i creates the MR based on the gathered information provided by the local misbehaviour detection service and optionally of other evidence obtained from other vehicles.
4. **Storage:** V_i stores MR to either share it with other nearby vehicles or to submit it later to the RS upon connectivity.

5. **Transmission**: After MR creation, V_i decides whether to share the MR with other nearby vehicles or to store it. If multiple MRs are available to send, V_i has to decide which ones to send and in which order.

During the LMDM process, the key functional component *State* is added, which is responsible for storing and managing information used by other parts of the system as outlined in ITS standards (IEEE Vehicular Technology Society, 2022). State manages three key factors:

- MR Creation: Allocates processor time and signing resources amid competing demands.
- Storage: Ensures MRs fit within available storage, prioritizing critical ones.
- Transmission: Manages limited connectivity, prioritizing essential MRs for timely transmission.

In the current state of the ITS standards (IEEE Vehicular Technology Society, 2022), every false message M_{sg} flagged as misbehaving is reported. However, not every M_{sg} should be separately reported as this would cause a significant network overhead particularly when the misbehaving is a result of a faulty component in its system. Consequently, the MR format allows for omitted MRs, which means that the Rep_{Veh} temporarily stops generating repeated MR for the exact Tar_{Veh} about the same misbehaviour after detecting it. Instead, it continues collecting relevant evidence over time. Once enough proof is gathered, the Rep_{Veh} generates a single, detailed MR to the RS. The protocol assumes that the RS is capable of prioritizing the quality and significance of the MR's content, rather than just counting how many MRs it receives. This method increases reporting efficiency and decreases redundant communications.

Process 2: Online Reporting (OR)

To send an MR to the RS, Rep_{Veh} may use different communication channels for reporting Tar_{Veh}. In line with TS 103 759 - V2.1.1 standards (European Telecommunication Standard Institute ETSI97, 2021), the following communication protocols are considered for establishing the connection between Vehicle-to-Infrastructure (V2I):

- DSRC short via RSU or a cellular network link (3G, 4G, or 5G).
- A wireless or wired connection at an electric vehicle charging station.
- A Wi-Fi hotspot that offers Internet access, such as in a parking lot or a private hotspot at home.
- Running the Vehicle On-Board Diagnostic (OBD) port and a diagnostic system at the inspection workshop or service garage.

Upon connectivity, the following sub-phases have to be done to complete the precess of the OR.

1. **RS Communication**: Vehicles establish a secure connection with the RS either via RSUs or directly. In order to achieve such a communication within the RS during the MR submission process, the ISO 15118 standard requires Transport Layer Security (TLS) function for secure communication between vehicle and infrastructure as mandatory. With TLS handshake, vehicles and RS are securely authenticated, and cryptographic algorithms (cipher suite parameters) are configured. These steps are utilised to generate the TLS master key to encrypt and decrypt the communication messages between vehicles and RS in order to achieve the secure communication (authentication, integrity, and confidentiality).

2. **MR Reporting**: Once the communication is verified, the reporting vehicle submits the stored MRs, this phase ensures that local evaluations feed into the global trust framework, enabling the RS to update the reputation and notify the rest of the network about detected misbehaving vehicles. Based on the offline observations discussed in Table 7.2, four reporting conditions are considered, as outlined in Table 7.3.

Table 7.3: Rep_{Vehs} Reporting Conditions and RS Actions.

Condition	**Definition**	**RS Action**
O(R)	Observing and reporting MR.	Considers the MR based on the Rep_{Veh}'s RV and corroboration with other MRs.
O(NR)	Observing misbehaviour but not generating a MR.	Relies on other Rep_{Vehs} with high RV to compensate for missed reporting.
O(NMR)	Not observing misbehaviour but generating MR.	Evaluates the Rep_{Veh}'s RV and checks aggregation from other reporters to detect inconsistencies.
O(NNMR)	Neither observing nor generating.	No action is taken, and the Rep_{Veh}'s RV remains unaffected.

In this study, based on the standard MR format illustrated in (IEEE Vehicular Technology Society, 2022), the MR frame is classified into three containers:

(a) *Header*: Includes the fundamental data that an MR should have such as MR generation time, $Rep_{\textbf{Veh}}$ id, $Tar_{\textbf{Veh}}$ id, and MR type.

(b) *Source*: Includes the misbehaviour results where the $Rep_{\mathbf{Veh}}$ flags the $Tar_{\mathbf{Veh}}$ if the received M_{sg} shows implausibilities.

(c) *Evidence*: Contains the $Tar_{\mathbf{Veh}}$ M_{sg} and the $Rep_{\mathbf{Veh}}$ M_{sg} or any M_{sg} from the neighbouring $Rep_{\mathbf{Vehs}}$ if believed helpful. The evidence could also include other supported information like a Local Dynamic Map (LDM), or direct sensor data from the $Rep_{\mathbf{Veh}}$ OBUs. The detailed evidence for misbehaviour vehicles that required by the MA is further explained in (Kamel et al., 2020).

Having outlined the main containers of the MR format, the focus shifts to the expected three versions of received MR by the RS based on this format:

- Base MR: This basic version includes only the Header and the source containers without any evidence.
- Beacon MR: In this version, the $Rep_{\mathbf{Veh}}$ includes a base MR and the suspicious $Tar_{\mathbf{Veh}}$ M_{sg} as evidence.
- Evidence MR: This version contains a detailed report with more complete misbehaviour information depending on the type of plausibility checks failure. For example, if the $Tar_{\mathbf{Veh}}$ failed the speed consistency, the $Rep_{\mathbf{Veh}}$ includes all related inconsistent M_{sg} in the "Evidence Container" for deeper investigation.

These MR versions support an efficient reporting process by allowing the RS to aggregate evidence and send a single comprehensive MR to the MA, reducing network overhead and ensuring accurate incident tracking.

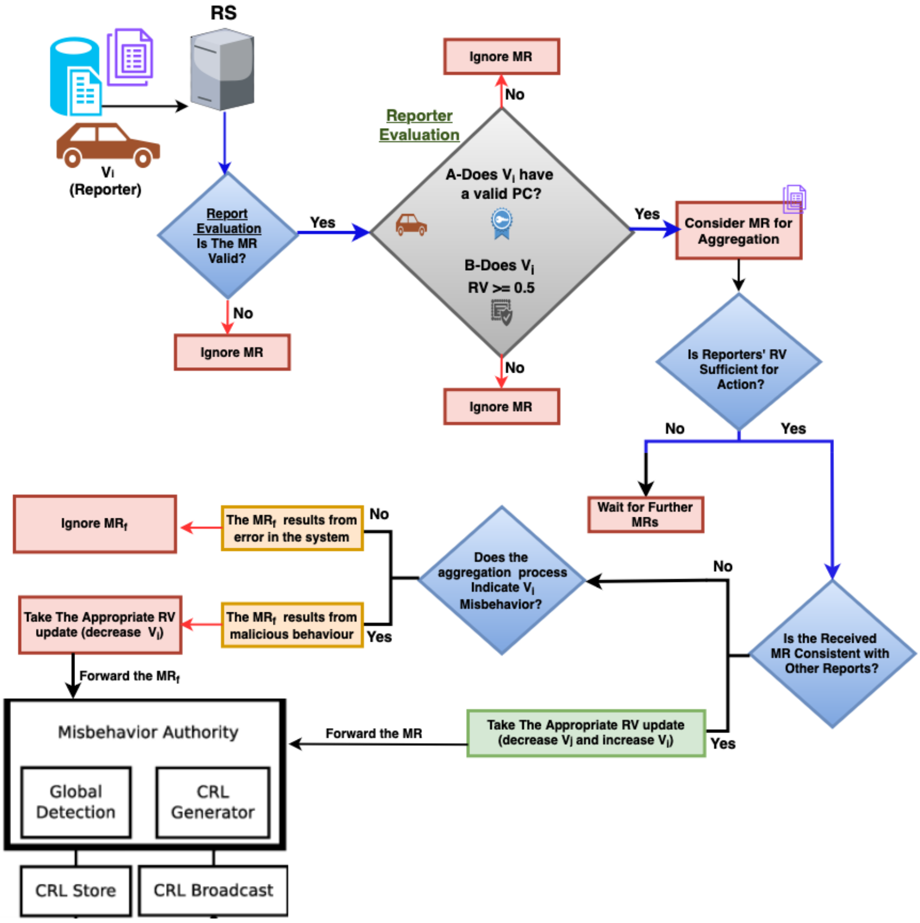

RS
V$_i$
(Reporter)
Report Evaluation
Is The MR Valid?
Yes
No
Ignore MR
Reporter Evaluation
Ignore MR
No
A-Does V$_i$ have a valid PC?
B-Does V$_i$ RV >= 0.5
No
Ignore MR
Yes
Consider MR for Aggregation
Is Reporters' RV Sufficient for Action?
No
Yes
Wait for Further MRs
Is the Received MR Consistent with Other Reports?
No
Yes
Does the aggregation process Indicate V$_i$ Misbehavior?
No
Yes
The MR$_f$ results from error in the system
The MR$_f$ results from malicious behaviour
Ignore MR$_f$
Take The Appropriate RV update (decrease V$_i$)
Forward the MR$_f$
Take The Appropriate RV update (decrease V$_i$ and increase V$_i$)
Forward the MR
Misbehavior Authority
Global Detection
CRL Generator
CRL Store
CRL Broadcast

Figure 7.5: Process 2: Online Reporting Illustration.

3. **RS Process:** The RS in the system, is a centralised entity that collects MRs from reporters, decides on the suitable reaction to make, and evaluates their credibility to determine the reputation scores and forwards verified MRs to the MA for further action, Figure 7.5 illustrates the OR process.

   Based on Figure 7.5, three main functions of the RS are defined as follows:

   - MRs Grouping and Structure: The RS collects all the MRs and then adds them to its database. This step would enable to access MRs using specific criteria. For instance, the RS can get all the

MRs accusing a certain pseudonym or all the MRs from a specific area. Those requests could be helpful during the analysis phase. Additionally, the RS filtering system aggregates similar MRs such as those showing speed inconsistencies.

- MRs Analysis and RS Actions: The RS analyses the MRs to output the correct reaction. Correct MRs mostly align with a Rep_{Vehs} past behaviour and match the majority consensus, while MR_f often deviates from or contradicts these patterns. The RS also employs outlier detection, temporal and spatial correlation checks, and monitors to identify inconsistencies or malicious intent in MRs. Table 7.4 outlines the classification of how incoming MRs are evaluated for potential misbehaviour Rep_{Vehs} based on various inconsistencies.

Table 7.4: MR_f Classification.

Class	**Purpose**	**RS Action**
1	Implausible MR values.	Checks if the MR values are realistic.
2	Consistency checks with previous MRs.	Compares a MR with earlier ones from the same Rep_{Veh}.
3	Validation against local knowledge.	Checks the MR against the vehicle's map or local data.
4	OBUs-based MR validation.	Compares the MR with the vehicle's own sensors.
5	Cross-MR consistency analysis.	Checks if the MR agrees with other MRs for the same event.

- RS Decision: A simple threshold method is proposed for the RS to trigger reaction levels based on a flexible MR count. While an accurate misbehaviour reaction is still a debated subject in the ITS, three levels of RS reaction for both the Rep_{Veh} and Tar_{Veh} are proposed, as shown in Table 7.5.

Table 7.5: Actions Triggered by the RS for Tar_{Veh} and Rep_{Veh}

Level	$Tar_{\mathbf{Veh}}$	$Rep_{\mathbf{Veh}}$
0	No action taken.	No action taken.
1	A warning is sent for misbehaving.	A warning is sent for MR_f.
2	The Tar_{Veh} RV is reduced.	The Rep_{Veh} RV is reduced.

4. **Blacklist and Penalty Enforcement**: Potentially misbehaving vehicles (Rep_{Veh} and Tar_{Veh}) will be reported to the MA. If the RV drops below the pre-set threshold, the RS develops a detailed MR and sends it to the MA within the SCMS. The MA decides on the seriousness level of the low RV and utilises misbehaviour detection algorithms to assess the situation and notify all participants regarding the detected misbehaviour in two stages of reaction:

   (a) Passive revocation: the Tar_{Veh} is blocked from requesting new certificates or the Rep_{Veh} is temporarily suspended from reporting privileges.

   (b) Active revocation: the Tar_{Veh}'s current certificates will be revoked, which is then sent to the CRL. The Rep_{Veh} will be a permanent ban from submitting MRs.

DRAMBR Privacy

As explained in the previous chapters, integrating the reputation system with the SCMS ensures privacy by employing Pseudonym Certificates (PCs) that hide actual identities. However, the question of when and how a PC change occurs remains unresolved. Numerous techniques have been proposed by scientific investigations to ascertain the location and pace of change of PCs (Babaghayou et al., 2020).

Mechanisms that focus on node-centric Misbehaviour Detection (MBD) require a consistent identity to effectively monitor and evaluate the behaviour of the Tar_{Veh}. However, privacy-preserving strategies based on PCs introduce identity changes, complicating accurate tracking. Therefore, considering an appropriate PCs change strategy, as outlined below, becomes essential to balancing privacy and accountability.

- Random: The PC has a predefined possibility of changing with each outgoing message.
- Disposable: The PC is used for a predetermined number of messages, such as beacons and warnings.
- Periodical: After a predetermined amount of time, the vehicle changes its PCs.
- Distance: After a predetermined number of kilometres, the vehicle changes its PCs.

7.3 DRAMBR Technical Implementation

This section outlines the adopted computational processes across the two stages of DRAMBR to establish a foundation for the experiment design and evaluation.

7.3.1 DRAMBR: Offline Evaluation

It is assumed that the system consists of N vehicles $\{V_1, V_2, \ldots, V_N\}$, where each vehicle communicates with others within the network. Let V_j be the Tar_{Veh} observed by the Rep_{Veh} V_i. V_i evaluates multiple messages, each containing an *Action-ID*, which uniquely identifies actions (e.g., initiate, update, cancel) as per ETSI EN 302 637-3 V1.2.1 standards (IEEE Vehicular Technology Society, 2022). The system associates each incident with an *Incident-ID* (I_{inc}) aligned with the *Action-ID*, to ensure consistent tracking and grouping of related messages.

Let RV_{V_i} represent the RV of vehicle i, where $i \in \{1, 2, \ldots, N\}$. RV_{V_i} is a continuous variable defined in the range $RV_{V_i} \in [0, 1]$. Thus, $RV_{V_i}(t) = 1$ implies that vehicle V_i is fully trusted at a specific time t, and $RV_{V_i}(t) = 0$ indicates complete distrust. An RV threshold is set as τ_{Rep}, each vehicle V_i makes an acceptance decision based on the RV:

$$\text{Msg Acceptance Decision} = \begin{cases} \text{Accept } M_{sg} \text{ from} V_j, & \text{if } RV_{V_j}(t) \geq \tau_{Rep} \\ \text{Ignore } M_{sg} \text{ from } V_j, & \text{if } RV_{V_j}(t) < \tau_{Rep} \end{cases}$$

After M_{sg} acceptance, if V_i identifies V_j as a misbehaving vehicle, the process of generating and encrypting a misbehaviour report MR is as follows:

1. Vehicle V_i generates a misbehaviour report MR regarding V_j.

2. The MR is symmetrically encrypted using a session key K_s, producing the ciphertext:
$$C = \text{Enc}_{K_s}(MR)$$

3. The session key K_s is encrypted with the RS's public key K^S_{pub}, resulting in:
$$K_s^* = \text{Enc}_{K_{\text{pub}}^{RS}}(K_s)$$

4. The ciphertext C is signed by V_i using its private key K^i_{priv}, yielding a digital signature:
$$\sigma_A = \text{Sign}_{K^i_{\text{priv}}}(C)$$

7.3.2 DRAMBR: Online Reporting

The reporting process consists of secure transmission of MRs from Rep_{Veh} to RS. RS verifies the MRs, checks correctness, and updates RVs for both Rep_{Veh} and Tar_{Veh} while keeping privacy by *PCs*. Figure 7.6 illustrates the multi-stage process adopted in the proposed system by incorporating different classification techniques to have an efficient MR evaluation.

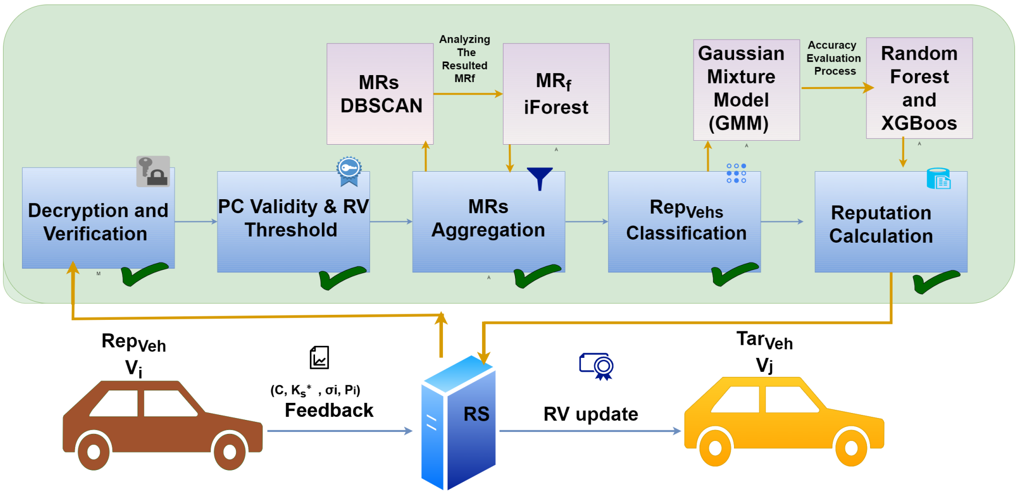

MRs DBSCAN
Analyzing The Resulted MRf
MR$_f$ iForest
Gaussian Mixture Model (GMM)
Accuracy Evaluation Process
Random Forest and XGBoos
Decryption and Verification
PC Validity & RV Threshold
MRs Aggregation
Rep$_{Vehs}$ Classification
Reputation Calculation
Rep$_{Veh}$ V$_i$
(C, K$_s$* , σi, Pi)
Feedback
RS
RV update
Tar$_{Veh}$ V$_j$

Figure 7.6: MR Evaluation.

1. **MR Decryption and Verification:** The RS performs the following operations after receiving the MR:

   (a) First, the RS decrypts K_s^* using its private key K_{priv}^S, retrieving the session key K_s:

   $$K_s = \text{Dec}_{K_{\text{priv}}^S}(K_s^*)$$

   (b) To retrieve the MR, the RS decrypts the ciphertext C

   $$MR = \text{Dec}_{K_s}(C)$$

   (c) Using the public key K_{pub}^i from PC, the RS verifies the signature σ_A , ensuring the integrity of the report:

   $$\text{Verify}_{K_{\text{pub}}^i}(C, \sigma_i)$$

2. **MR Preprocessing and Acceptance Criteria:** In this step the MRs are assessed by filtering out the invalid certificates and low-RV Rep_{Vehs} to ensure that only valid, reliable, and unique MRs are considered in further analysis.

   (a) The RS checks V_i certificate:

   $$\text{The MR from } V_i \text{ is accepted} \iff pc = 1$$

   $$pc = \begin{cases} 1 & \text{if } V_i \text{ has a valid certificate} \\ 0 & \text{if } V_i \text{ has an invalid certificate} \end{cases}$$

(b) The RS checks V_i RV:

$$\text{The MR from } V_i \text{ is accepted} \iff RV \geq \tau_{Rep}$$

3. **MRs Grouping Using DBSCAN**

This step identifies clusters of consistent MRs that likely reflect genuine events. The clustering algorithm: Density Based Spatial Clustering of Applications with Noise (DBSCAN) is used to identify clusters in a dataset based on the density of data points. DBSCAN does not require a predefined number of clusters, which making it particularly useful in scenarios with unknown cluster sizes or irregularly shaped clusters (Nathi, 2024).

In the conducted scenario, the RS follows this step to set the ground truth of what occurred in offline communications without relying on real-time infrastructure support. To illustrate, based on two parameters DBSCAN groups data points into clusters:

- **Epsilon (ϵ)**: The maximum distance between two points for them to be considered neighbours.
- **Minimum Points (*minPts*)**: The minimum number of points required to form a dense region (a cluster).

Figure 7.7 illustrates the DBSCAN idea as follows:

- **Core Points (red points)**: These have at least *minPts* neighbours within ϵ-distance.
- **Border Points (yellow points)**: These are within ϵ-distance of a core point but have fewer than *minPts* neighbours.
- **Noise Points (blue points)**: These do not meet the density criteria and are treated as outliers.

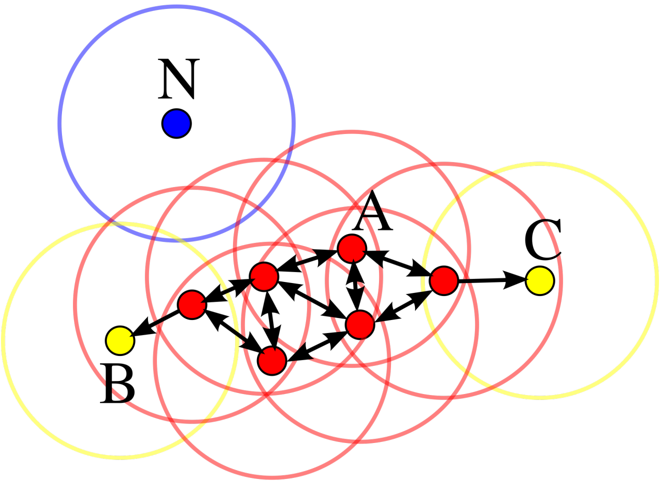


Figure 7.7: Illustration of DBSCAN.

Source: (Ester et al., 1996)

The DBSCAN process is adopted in the proposed system to validate all the MR generated in the offline communication. Hence, the RS can establish the ground truth regarding all the events; the following steps are applied:

(a) *Incident ID:* First, the MRs will be grouped based on their *Incident ID* (I_{inc}), which ensures that only MRs that are relevant to the same event are processed together:

$$R_{I_{\text{inc}}} = \{MR_i \mid I_i = I_{\text{inc}}\} \tag{7.1}$$

Each group $R_{I_{\text{inc}}}$ corresponds to a unique incident, isolating the observations related to that incident.

(b) *DBSCAN Inputs:* Within each group $R_{I_{\text{inc}}}$, DBSCAN is applied to identify consistent clusters of reports.

- **Feature set:** $x_i = [L_i, T_i]$, where:
  - L_i: Location of the Rep_{Veh}.
  - T_i: Timestamp of the MR.

- **Parameters:**
  - ϵ_L: Spatial threshold for proximity.
  - ϵ_T: Temporal threshold for proximity.
  - *minPts*: Minimum number of reports required to form a cluster.

Reports MR_i and MR_j within $R_{I_{\text{inc}}}$ are considered part of the same cluster $G_{I_{\text{inc}},k}$ if:

$$\|L_i - L_j\| \leq \epsilon_L \quad \text{and} \quad |T_i - T_j| \leq \epsilon_T \tag{7.2}$$

Reports that do not meet these criteria or do not belong to any cluster are treated as *noise* ($N_{I_{\text{inc}}}$).

Outputs:

- **Clusters ($G_{I_{\text{inc}},k}$):** Groups of MRs consistent in location and time, representing reliable observations.
- **Noise ($N_{I_{\text{inc}}}$):** MRs flagged as outliers (MR_f), which may indicate malicious or erroneous behaviour.

(c) *Determining Ground Truth:* For each cluster $G_{I_{\text{inc}},k}$, the following steps are performed:

1. Majority Voting for Reported Status ($S_{I_{\text{inc}},k}$): The dominant reported status $S_{I_{\text{inc}},k}$ (e.g., “accident” or “no accident”) is determined using:

$$S_{I_{\text{inc}},k} = \arg\max_s \left(\text{Count of } S_i = s \text{ in } G_{I_{\text{inc}},k}\right) \tag{7.3}$$

2. Confidence Aggregation for Ground Truth: In this step, the system calculates the cluster's confidence based on the Reporter's RV. The confidence of the majority-reported status $S_{I_{\text{inc}},k}$ within a cluster $G_{I_{\text{inc}},k}$ is calculated as follows to assess the reliability of the cluster:

$$\text{Confidence}(S_{I_{\text{inc}},k}) = \frac{\sum_{MR_i \in G_{I_{\text{inc}},k} \text{ and } S_i = S_{I_{\text{inc}},k}} C_i}{\sum_{MR_i \in G_{I_{\text{inc}},k}} C_i} \tag{7.4}$$

Where:

- The numerator aggregates the confidence scores C_i of reports within the cluster that align with the majority-reported status $S_{I_{\text{inc}},k}$.
- The denominator aggregates the total confidence scores of all reports in the cluster.

3. Final Decision: If $\text{Confidence}(S_{I_{\text{inc}},k}) \geq \text{Threshold}$, $S_{I_{\text{inc}},k}$ is accepted as the ground truth for incident I_{inc}.

This step ensures that only verified and consistent observations are used to analyse Rep_{Vehs} behaviour and update their RVs.

4. **Outlier Detection Using Isolation Forest for Anomaly Detection.**

After DBSCAN groups reports into clusters and flags noise points, Isolation Forest *(iForest)* refines this process by detecting anomalies (e.g., malicious or erroneous reports) within each cluster $G_{I_{\text{inc}},k}$ (Vinita and Vetriselvi, 2023; Ripan et al., 2021). This step works on the output of DBSCAN clusters and focuses on deeper, feature-based anomaly detection. iForest distinguishes between mild anomalies and extreme outliers. The input is each $G_{I_{\text{inc}},k}$ cluster from DBSCAN. The iForest calculates the anomaly score $s(x, n)$ for each report MR_i.

Path Length: Define $h(x)$, the number of splits required to isolate point x.

Anomaly Score for MR_i:

$$s(x,n) = 2^{-\frac{h(x)}{c(n)}}, \quad c(n) = 2H(n-1) - \frac{2(n-1)}{n}, \tag{7.5}$$

where:

- $H(x)$ is the harmonic number measures the number of steps or splits to isolate x
- n is the sample size,
- $c(n)$ normalizes the path length.

Outlier Classification:

MRs with:

$$s(x,n) > \tau \tag{7.6}$$

are classified as outliers (potential MR_s), where τ is the threshold.

Output: Classification of MR_f as outliers (anomalies) or inliers (consistent).

5. **Gaussian Mixture Model (GMM) for MR Classification**

Model the MR features $\mathbf{x} = [RV, \delta_L, \delta_T]$ using a Gaussian Mixture (Wan et al., 2019):

$$p(\mathbf{x}) = \sum_{k=1}^{K} \pi_k \mathcal{N}(\mathbf{x} \mid \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k), \tag{7.7}$$

where:

- π_k is the mixing weight (sum to 1),
- $\boldsymbol{\mu}_k$ is the mean vector,
- $\boldsymbol{\Sigma}_k$ is the covariance matrix.

The posterior probability that $\mathbf{x}$ belongs to component k is given by:

$$\gamma_k(\mathbf{x}) = \frac{\pi_k \mathcal{N}(\mathbf{x} \mid \boldsymbol{\mu}_k, \boldsymbol{\Sigma}_k)}{\sum_{j=1}^{K} \pi_j \mathcal{N}(\mathbf{x} \mid \boldsymbol{\mu}_j, \boldsymbol{\Sigma}_j)}. \tag{7.8}$$

Clustering Decision

- $k = 1$: Honest $Rep_{\mathbf{Vehs}}$.
- $k = 2$: Malicious $Rep_{\mathbf{Vehs}}$.
- $k = 3$: Erroneous$Rep_{\mathbf{Vehs}}$.

Output: Labels for $Rep_{\mathbf{Vehs}}$: Honest, Malicious, Erroneous.

6. **Ensemble: Random Forest and XGBoost**

A combination of Random Forest and XGBoost is used to refine the classification of MRs (Ramraj et al., 2016; Joharestani et al., 2019). These steps process the features generated during the earlier stages to provide a binary classification of MRs.

Previous Steps

- **DBSCAN:** Set the ground truth for the actual event and clusters of MRs based on spatial and temporal proximity.
- **Isolation Forest (iForest):** iForest isolates potential anomalies within the identified clusters and flags suspicious reports.

- **G**MM: Models the distribution probability of misbehaviour, separating normal and abnormal patterns.

These steps then provide the input feature set for this step, defined as:

$$\mathbf{x} = [RV, \delta_L, \delta_T, s(\mathbf{x}, n)], \tag{7.9}$$

Where: $s(\mathbf{x}, n)$: Relationships between the data points (e.g., report similarity).

Classification Models

- **Random Forest:** Random Forest aggregates predictions from multiple decision trees. Each tree T_i independently classifies the data, and the final decision is made via a majority vote:

$$f_{\text{RF}}(\mathbf{x}) = \text{Majority Vote}(T_1(\mathbf{x}), T_2(\mathbf{x}), \ldots, T_m(\mathbf{x})). \tag{7.10}$$

- **XGBoost:** XGBoost minimizes a custom loss function:

$$L = \sum_i l(y_i, \hat{y}_i) + \Omega(f), \tag{7.11}$$

  Where:

  - $l(y_i, \hat{y}_i)$: Loss function (e.g., log loss) comparing predictions $\hat{y}_i$ with actual labels y_i,
  - $\Omega(f)$: Regularization term penalizing overly complex models, improving generalization.

- **Combined Prediction:** Predictions from both models are combined using a weighted average:

$$f_{\text{final}}(\mathbf{x}) = w_{\text{RF}} f_{\text{RF}}(\mathbf{x}) + w_{\text{XGB}} f_{\text{XGB}}(\mathbf{x}), \tag{7.12}$$

  where w_{RF} and w_{XGB} are the respective weights for Random Forest and XGBoost.

Output: In this step, the final decision for each MR will be one of the following:

- **Honest:** The MR is correct, reflecting an honest behaviour of the Rep_{Veh} and true Tar_{Veh} misbehaviour.
- **Malicious:** The MR is false, generated and submitted intentionally, reflecting malicious behaviour of the Rep_{Veh} and false Tar_{Veh} misbehaviour.
- **Erroneous:** The MR_f is wrong because of mistakes in the Rep_{Veh} system.

7. **RV Update**

Weighted Increment/Decrement Based on Decision.

For each $Rep_{veh(i)}$, update the RV_i:

$$RV_i^{\text{new}} = \begin{cases} RV_i + \Delta_{\text{pos}} & \text{if Honest } Rep_{\text{Veh}} \text{ (True Positive)}, \\ RV_i - \Delta_{\text{neg}} & \text{if Malicious } Rep_{\text{Veh}}, \\ RV_i & \text{if Erroneous Report.} \end{cases}$$

where Δ_{pos} and Δ_{neg} are predefined step sizes.

7.4 DRAMBR Experimental Evaluation

This section discusses the simulation scenario, implementing the proposed DRAMBR system to measure its accuracy in misbehaviour reporting process. First, the experiment description is introduced, highlighting the core concept. Then an outline of the simulation environment is provided, setting the stage for the experiment setup.

7.4.1 Experiment Description

The main focus in the conducted experiment is analysing the MRs generated by Rep_{Vehs} during communications in offline settings. Different scenarios are designed, as explained below, to serve as trigger events for reporting the misbehaviour generated by the Tar_{Vehs}. These scenarios set the stage for the evolution process and enable the identification of further misbehaviour activities in disconnected areas during emergencies.

Three scenarios are considered to simulate realistic events that could lead to the generation of MRs:

- Accident Occurs *(ACD-OCC)*
- Accident Absent *(ACD-ABS)*
- Accident Resolved *(ACD-RSL)*

Table 7.7 below summarizes the Rep_{Veh} behaviours in each scenario and the types of MRs they trigger:

Table 7.6: Accident Scenarios and Triggered Misbehaviour Reports (MRs)

ACD	$Rep_{\mathbf{Veh}}$	I_{inc}	**Message Content**	**Triggered MR**
OCC	Honest	IR-101	”Accident detected at location X, proceed cautiously.”	Reports malicious vehicles for denying the accident.
	Malicious	IR-101	”No incident at location X, road is clear.”	Reports honest vehicles for claiming an accident.
ABS	Honest	IR-201	”No incident at location X, road clear.”	Reports malicious vehicles for claiming an accident.
	Malicious	IR-201	”Accident detected at location X, avoid area.”	Reports honest vehicles for denying the accident.
RSL	Honest	IR-301	”Incident resolved at X, road clear.”	Reports malicious vehicles for claiming the incident persists.
	Malicious	IR-301	”Incident still active at X, avoid area.”	Reports honest vehicles for claiming resolution.

7.4.2 Simulation Setup

This section provides the detailed simulation setup for the three scenarios, including the configurations, parameters, and communication dynamics used to analyse the generated MRs. To simulate realistic vehicular movements, the experiment is started by importing a map and integrating it into the Simulation of Urban Mobility (SUMO) environment (Lopez et al., 2018). The OpenStreetMap is used to import a map from the rural area of Peak District, as shown in Figure 7.8 (Haklay and Weber, 2008). In this step, the three scenarios are implemented to see how vehicles evaluate each other’s behaviours and generate MRs based on observed misbehaviour without connectivity.

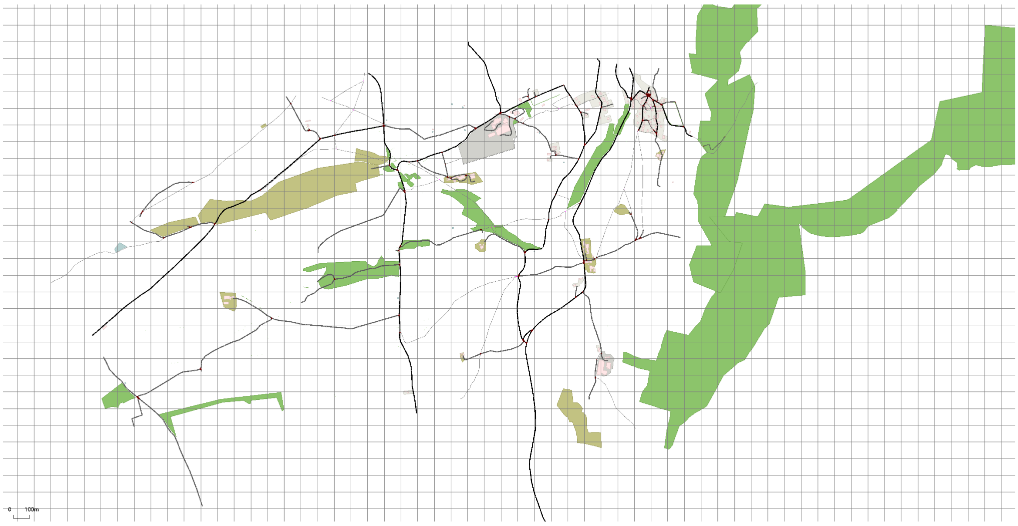


Figure 7.8: Simulated Map of Peak District Area.

Every vehicle has the DSRC/WAVE (IEEE 802.11p) protocol, a common wireless communication interface. SUMO simulation generates floating car data (FCD) output, which captures vehicle-specific metrics such as position, speed, angle, and other details at each timestep. This raw data is collected and saved in an FCD file, which serves as the primary dataset for analysing vehicular behaviours and identifying potential misbehaviour events. The FCD file is subsequently processed to extract relevant information, and the data is stored in a CSV file. This CSV file initially contains information about misbehaviour reports, including attributes such as the reporter ID, timestamp, and location. The simulation parameters in this experiment are given in Table 7.7.

Table 7.7: DRAMBR Simulation Details.

Parameter	**Value**
Traffic Simulator	SUMO 1.21.
Simulation Area (Rural)	4*4 km^2.
Network Configuration	Realistic layout.
Communication Standard	(DSRC) IEEE 802.11. P.
Road side Unites (RSU)	0.
Simulation Time	1800 s.
Event Duration	900 s.
Number of Vehicles	100.
RV Threshold (τ_{Rep})	0.5.
MAC Protocol	IEEE 1609.4.
Output Files	tripinfo.xml.

The RV is set to 0.5 to align with established reputation standards, which balance the trade-off between maintaining system reliability and minimizing false positive rates. In reputation systems, a threshold of 0.5 is widely adopted because it reflects the same probability of an entity being trustworthy or otherwise; hence, it is a balancing point for any decision (Jain and Singh, 2022). In vehicular networks, vehicles with trust values higher than 0.5 may be considered trustworthy when forwarding data, while lower values indicate distrust. Similarly, temporal network studies have employed a 0.5 credibility threshold to evaluate trustworthiness effectively (Lui, 1998). Although 0.5 is a standard choice, its value may be adjusted based on system requirements or empirical data (Hancock et al., 2022).

Table 7.8: DRAMBR Pipeline.

Step	Objective	Methods	Output
Grouping	Group MRs by time/location	DBSCAN	MR Clusters (G1, G2, ...)
Detection	Detect anomalous MRs	Isolation Forest	Outliers and Inliers
Rep_{Vehs} Classification	Classify Rep_{Vehs} probabilistically	Gaussian Mixture Model (GMM)	Honest, Malicious, Erroneous
Final Classification	Robust decision-making	Ensemble (Random Forest + XGBoost)	Final MR Labels

The resulting MRs are organised into three files, each file is associated with a specific event: : (ACD-OCC), (ACD-ABS), and (ACD-RSL). The data in each file is filtered to remove redundancy, ensuring that only relevant and unique MRs are retained. Subsequently, processing is carried out to the MRs for further analysis by implementing the DRAMBR system following the steps illustrated in table 7.8.

7.5 Results and Discussion

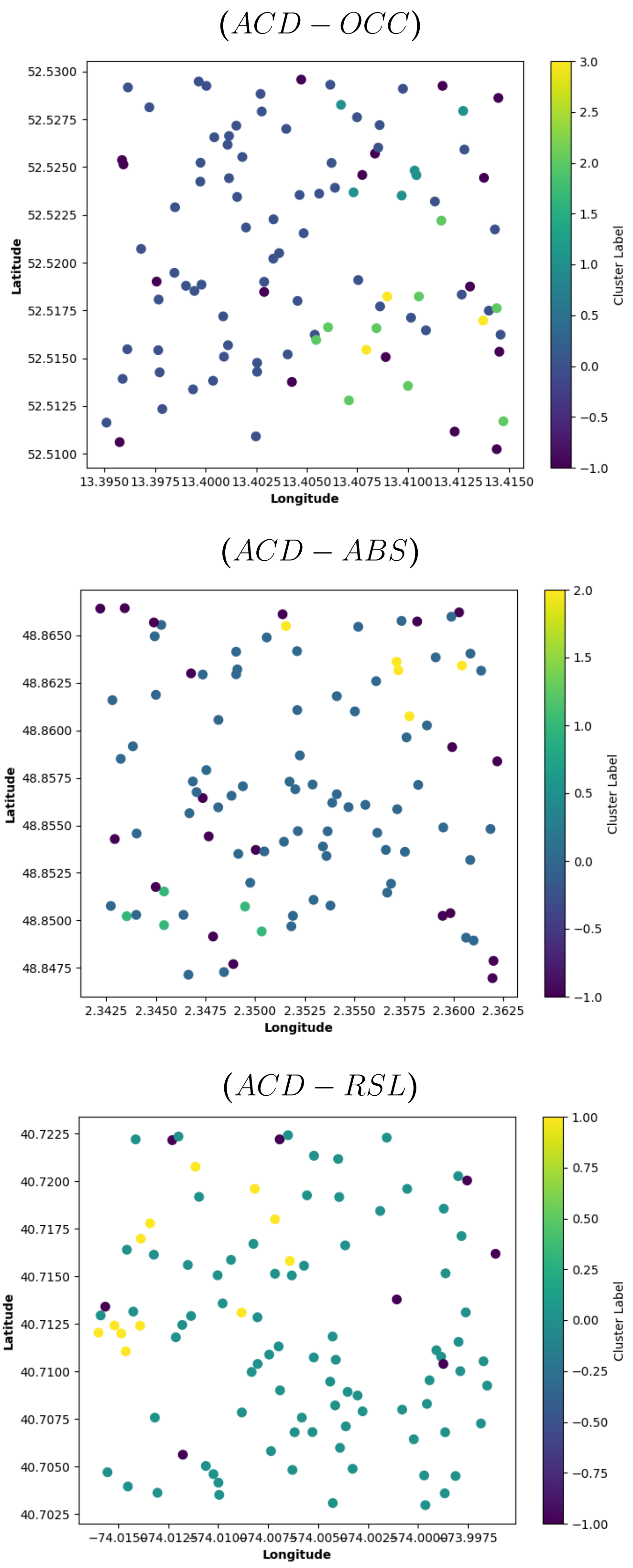
Based on the experiments described above, this section evaluates the performance and accuracy of the proposed DRAMBR in identifying false MRs under various scenarios. First, the results obtained from applying DBSCAN are presented. The outputs from this stage are essential for the subsequent stage, involving the implementation of the iForest methodology to evaluate the findings from the DBSCAN analysis. Following this, the aggregated results are analysed using GMM to finalize the reporter's behaviours. After that, the combined Random Forest and XGBoost methodologies are implemented to estimate the effectiveness and the accuracy of the results before moving to the final stage of updating the reputation.

7.5.1 Results From Applying DBSCAN

DBSCAN serves as the main step when the RS receives a large number of MRs regarding misbehaviour in offline scenarios. Its role is to analyse these MRs and group them into clusters that represent consistent patterns.

Figure 7.9 shows the DBSCAN results of clustering the received 100 MRs in each scenarios. In $ACD - OCC$, multiple distinct clusters (blue and green) represent consistent groups of MRs agreeing on the accident's occurrence. Noise points (yellow) are conflicting MRs that cannot fit into any cluster.

In $ACD - ABS$ and $ACD - RSL$, clustering is less distinctive, with a higher number of noise points and smaller cluster sizes, indicating higher variability or disagreement among the reporters. This then underscores the difficulties inherent in establishing the truth behind scenarios when reporting is more inconsistent.



$(ACD - OCC)$

$(ACD - ABS)$

$(ACD - RSL)$

Figure 7.9: DBSCAN Clustering Results for Different Scenarios: $ACD - OCC$, $ACD - ABS$, $ACD - RSL$.

- DBSCAN $ACD - OCC$

  In $ACD - OCC$, DBSCAN identified 5 clusters; the largest cluster, Cluster 0, contained 65 MRs. In total, it flagged 17 MRs as noise out of 100 MRs, which accounts for 17% of all the MRs. This represents moderate consistency among the Rep_{Vehs} since 83% of the MRs fell into meaningful clusters.

- DBSCAN $ACD - ABS$

  In the second scenario $ACD - ABS$, DBSCAN grouped the MRS into 4 clusters, with Cluster 0 dominating by including 70 MRs. However, this scenario also shows a high level of noise, with 20 MRs flagged as outliers, accounting for 20% of the total.

- DBSCAN $ACD - RSL$

  In the case of the final scenario $ACD - RSL$, DBSCAN identified 3 clusters, with Cluster 0 containing 80 reports. Only 8 MRs were classified as noise out of 100 MRs, which means 8% of the total. The scenario shows the highest reliability in reporting, as 92% of the received MRs fall well within the identified clusters, showing strong agreement among the Rep_{Vehs} .

Generally, DBSCAN effectively segregates consistent MRs into clusters while identifying noise points for further refinement using Isolation Forest to distinguish between serious anomalies and erroneous reports.

7.5.2 Results From Applying Isolation Forest

Figure 7.10 displays the outcomes of the iForest applied specifically to the noise points identified in the DBSCAN step across three scenarios: $ACD-OCC$ with 17 points, $ACD-ABS$ with 20 points, and $ACD-RSL$ with 8 points. Each sub-figure illustrates the latitude and longitude of the reports, overlaid with the iForest's classification results, represented by the outlier scores (colour gradient).

- iForest $ACD - OCC$

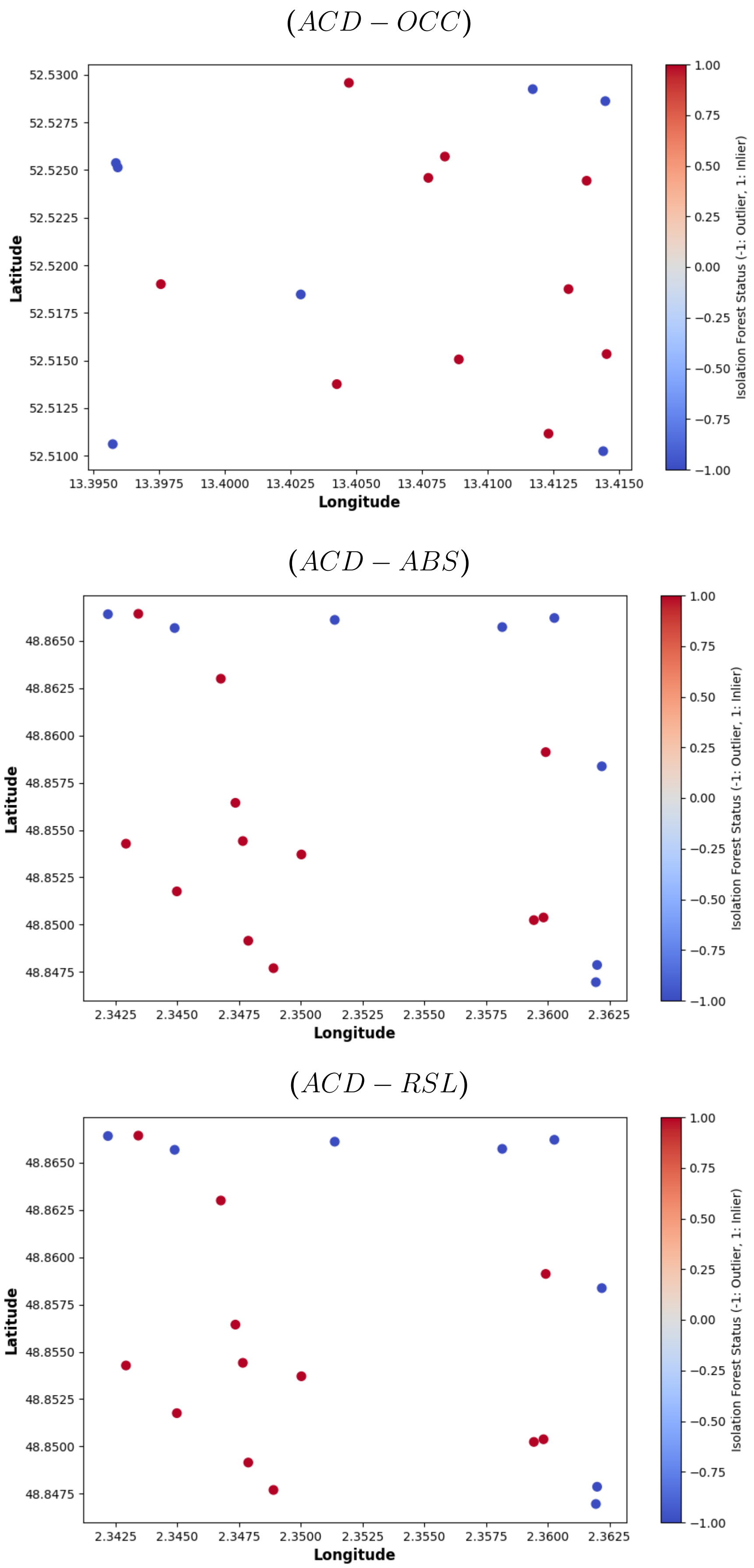
  For the first scenario $ACD-OCC$, the iForest refined the resulted 17 noise points from DBSCAN by classifying a subset as outliers (blue) representing 7 MRs, and the rest as inliers (red) with 10 MRs. The outlier percentage in this step is 41.18%, this demonstrates how the iForest narrows down potential serious anomalies within the initially noisy MRs, helping identify MRs that significantly deviate from the expected behaviour.

- iForest $ACD - ABS$

  For the second scenario $ACD-ABS$: the iForest refined the 20 noise points from DBSCAN by classifying a subset as consistent inliers (red) with 12 MRs, and some MRs that were classified as anomalies (blue) 8 MRs. The outlier percentage in this step is 40%.

- iForest $ACD - RSL$

  The third scenario $ACD-RSL$ exhibits a moderate balance of inliers (red) equal to 5 MRs and outliers (blue) equal to 3 MRs, which is representing a percentage of 37.5% of outliers. The iForest aids in detecting misleading or erroneous MRs in a scenario where there might be conflicting observations about the resolution of an event.



$(ACD - OCC)$

$(ACD - ABS)$

$(ACD - RSL)$

Figure 7.10: Isolation Forest Results on DBSCAN Noise Points.

The iForest results illustrate the efficacy of further examining noise points to distinguish serious anomalies from less critical deviations. This layered approach enhances the RS reliability of misbehaviour detection and decision-making regarding the received MRs. To further distinguish between honest, malicious, and system error $Rep_{\mathbf{Vehs}}$, the following section discusses the results generated from using the Gaussian Mixture Model (GMM) that focuses on classifying and identifying the $Rep_{\mathbf{Vehs}}$.

7.5.3 Gaussian Mixture Model (GMM)

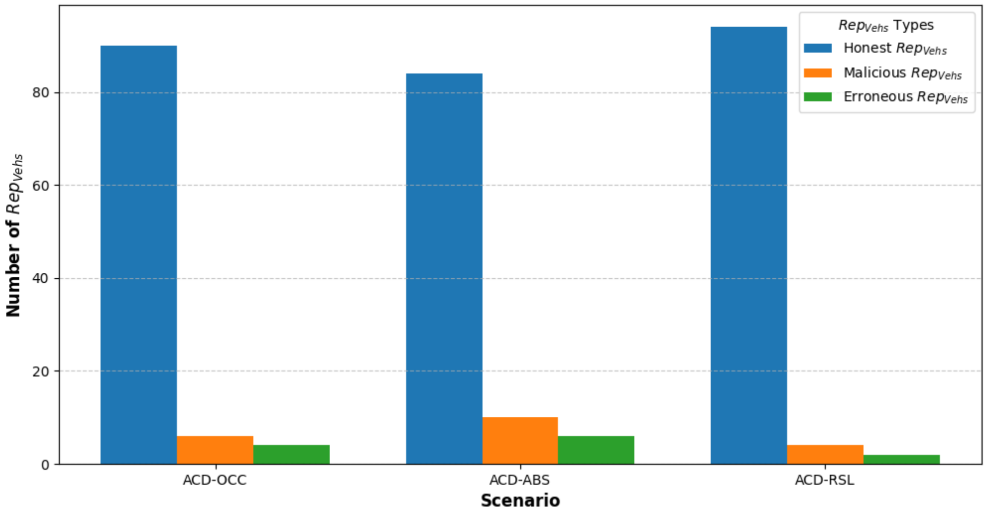


Figure 7.11: Reporter Classification Results.

Figure 7.11 shows the classification results generated from the Gaussian Mixture Model (GMM) to correctly identify the Rep_{Vehs} types in all three scenarios: $ACD-OCC$, $ACD-ABS$, and $ACD-RSL$. The results categorize Rep_{Vehs} into three types: Honest, Malicious, and Erroneous Rep_{Vehs}.

- Honest Rep_{Vehs}: In all three scenarios, honest Rep_{Vehs} Represented by the (Blue Bars) show The majority of the cases, with approximately 80 Rep_{Vehs} for each scenario which indicates a consistent pattern of correct reporting across scenarios.

- Malicious Rep_{Vehs}: As shown in the (Orange Bars), a small proportion of Rep_{Vehs} are identified as malicious, These Rep_{Vehs} intentionally submit MR_f with a consistent number across scenarios, ranging from approximately 6 to 10.

- Erroneous Rep_{Vehs}: This is the smallest group, represented by the (green bars). These Rep_{Vehs} submitted incorrect reports MR_f, resulted from an unintentional error, and were not indicative of deliberate misbehaviour. The false in these MRs is due to sensor faults or environmental errors. The number of Rep_{Vehs} with erroneous data differs slightly, with a minimal count observed in each scenario.

In this classification, the proposed system's efficiency is highlighted in distinguishing between honest, malicious, and erroneous behaviour, helping the RS maintain accuracy and filter out potentially disruptive or inaccurate reports.

7.5.4 DRAMBR Accuracy

In this ensemble classification, the DRAMBR's accuracy is evaluated across the three scenarios, as well as the overall system performance. The Random Forest and XGBoost models are combined to analyse the accuracy in two ways:

1. **Noise-based Accuracy:** Focused only on noise points refined by DBSCAN and Isolation Forest. This classification results in 72%.
2. **Full System Accuracy:** Includes all MRs (honest and noise) across all scenarios. This evaluation results in 98%.

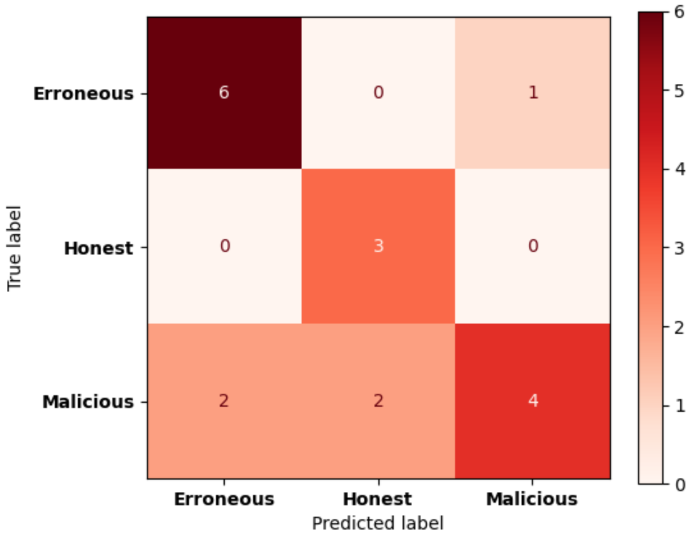


Figure 7.12: Confusion Matrix Representing DRAMBR Performance in Noise-Based Accuracy.

Figure 7.12 illustrates the noise based classification with 72% accuracy from Random Forest and XGBoost highlights the performance of DBSCAN iForest, and GMM models applied to the noise points.

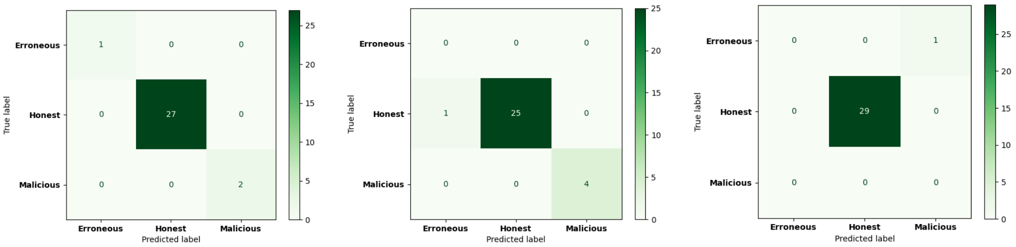


Figure 7.13: Confusion Matrix Representing DRAMBR Performance in $ACD - OCC$ (**Left**), $ACD - ABS$(**Middle**), $ACD - RSL$(**Right**).

The sub-graphs in Figure 7.13, show the Random Forest and XGBoost results in the three scenarios, achieving a total accuracy of 98%, which measures the effectiveness of the entire system.

The total system accuracy, as shown in Table 7.9 reflects the system's overall ability a to classify MRs and Rep_{Vehs} correctly across the three scenarios, including:

1. Consistent MRs from DBSCAN (True Positives).

2. Refined classifications of noise points through iForest and GMM.

Table 7.9: Performance Accuracy Across Scenarios

Scenario	$ACD-OCC$	$ACD-ABS$	$ACD-RSL$	**Overall**
MRs	100	100	100	300
Consistent	83	80	92	255
Noise	17	20	8	45
Precision	100	100	97	99
Recall	100	97	97	98
F1-Score	100	98	97	98
Accuracy	100	97	97	98

The results in Figure 7.14 compare accuracy, precision, recall, and F1-score in each scenario and the overall system, highlighting the system's robustness in distinguishing between honest, malicious, and erroneous reporters across all scenarios. The (ACD-OCC) scenario demonstrates the system's ability to achieve perfect classification. The other scenarios (ACD-ABS and ACD-RSL) show consistently high accuracy of 97%, even under varying conditions.

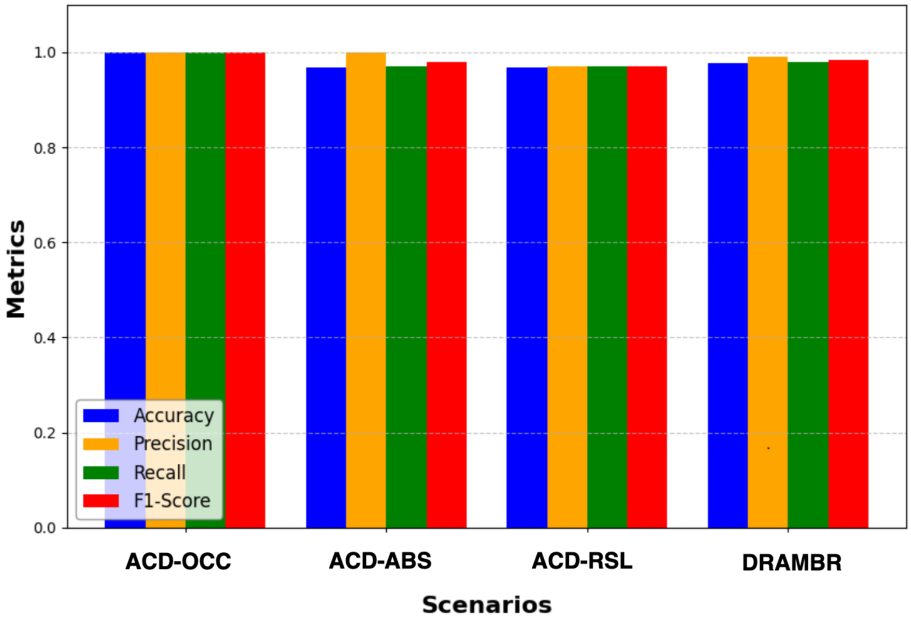


Figure 7.14: Accuracy, Precision, Recall, and F1-Score Across Scenarios and Overall System

The overall accuracy of 98% indicates that the DRAMBR system correctly classified approximately most of the MRs across all scenarios. It is worth noting that as the system benefits from larger datasets to make more reliable decisions, the system accuracy improves with an increasing scale of reporters. The results demonstrate how the system effectively distinguishes between honest, malicious, and erroneous reporters. This approach ensures accurate reputation updating for both reporters and targets, enhancing trust and accountability in disconnected vehicular networks, as it ensures reliable decision-making even under constraints.

7.6 Conclusion

The study has presented a novel multi-layered scheme for accurately detecting and classifying misbehaviour in V2V networks. Through its two phases, the proposed DRAMBR has effectively identified and mitigated misbehaviour by leveraging local observations and neighbouring feedback in offline settings, later consolidating reports with a centralised RS upon connectivity. The system leverages advanced classification techniques to manage misbehaviour reports and identify patterns in each report to effectively distinguish between honest, malicious, and erroneous reporters which ultimately contribute to the reliability and resilience of vehicular communication systems in challenging offline scenarios to assign reputation more accurately to both the reporters and the targeted vehicles.

The findings demonstrate the DRAMBR effectiveness in reducing false reporting which improves decision accuracy, ensures reliable detection of misbehaviour, and supports the RS's ability to maintain system integrity. Adopting DRAMBR results in enhanced V2V communication reliability, and ensuring a safer network in infrastructure-limited environments.

Chapter 8

Conclusions and Future Research

8.1 Summary of Achievements

Maintaining secure communications and safeguarding against attacks is crucial in vehicular networks, to ensure trusted message exchange among vehicles V2V and between vehicles and infrastructure V2I. However, the sparse infrastructure in some regions exacerbates connectivity issues, complicating the dissemination of critical messages, especially in emergencies. The lack of continuous network coverage creates a window of opportunity for various attack scenarios that might engage in fraudulent behaviours and mislead other vehicles within the same area. Thus, establishing reliable communication and enabling a trustworthy relationship between vehicles in disconnected areas is exceptionally challenging.

In light of this discussion, the thesis's main contribution focuses on strengthening the confidence and trust between vehicles in disconnected areas to increase decision-making accuracy in the presence of attacks under emergencies. The research proposed, implemented, and evaluated a novel reputation-based system integrated with the SCMS to accomplish this objective. The foundation of this research was built on the literature review that exploring three critical areas:

1. VANETs: Discussed the main concepts of vehicular networks and the unique challenges in disconnected areas.
2. Security and Privacy: Explored the certification systems like the SCMS to show their effectiveness in using certificates to authenticate the exchanged messages and ensure privacy in V2V communications.
3. Trust and Reputation Mechanisms: Reviewed different trust and reputation approaches in vehicular networks, pointing out the shortcomings in addressing misbehaviours in the research context.

These insights shaped the development of a reputation-based system and set the stage for the innovative achievements as outlined below:

- **Reputation Framework Development**

  Developed a reputation framework by extending the SCMS with a reputation server. Vehicles can securely retrieve and update their recent reputations, which then can be used in critical situations with low connectivity, ensuring accurate and reliable trust management while maintaining privacy.

- **Novel Signature Scheme**

  Proposed the Pre-Signature scheme, which enables an appropriate balance between trust, security, and privacy without breaking standards. The scheme allows reputation to be used even when vehicles are pseudonymous and out of connectivity range.

- **Simulation Tool Development**

  Integrated different simulation tools to design customised scenarios to evaluate the proposed reputation system under various conditions, such as Sybil attacks and accidents in offline communication.

- **Accurate Decision-Making Logic**

  Enhanced decision accuracy by combining reputation and certificates to accept legitimate messages and reject the false ones under attack and accident scenarios. Vehicle decision accuracy improves by 36% in accident scenarios and 44.4% in no-accident scenarios during V2V communications in a rural environment.

- **Misbehaviour Reporting Scheme**

  Introduced and evaluated an accurate misbehaviour reporting system (DRAMBR). By integrating multilayer mechanisms like DBSCAN, the reputation server can validate the misbehaviour reporting process from offline detection to online reporting. With 98% accuracy, the mechanism efficiently classifies misbehaviour reports and distinguishes between honest, erroneous, and malicious reporters.

- **Foundations for Future Research and Applications**

  Bridged the gap between trust theory and its application in vehicular networks, thus providing actionable insights with a flexible system that can adapt to the evolving vehicular communication technologies.

8.2 Limitations of The Research

Although this thesis has contributed valuable insights into enhancing trust, privacy, and security V2V communications in disconnected areas, it is important to recognize certain inherent limitations in the proposed solutions.

- **Simulation Environment Constraints**

  Given that the assumption is laid on V2V communications in disconnected areas, a practical set of simulation tools that may replicate the assumption is selected. These tools are developed for vehicular communications and networks that allow the design of realistic vehicular environments to evaluate the reputation system properly.

  The study derives substantial insights into system behaviour through simulation environments. However, it is hard to thoroughly represent all the actual conditions through a simulation. Dynamic characteristics, such as the limitations in OBUs, different levels of vehicle automation, and varying environmental conditions like weather and terrain, may affect the performance of the proposed approach in VANETs. Besides, some connectivity challenges, like fluctuating signal strength, interference, and instability of the network, make it hard to measure the real impact of intermittent disconnections in real-world scenarios. In addition, assumptions about network latency, packet loss, and device interoperability were made to make the simulation uncomplicated. In most practical application scenarios, these technological variables are usually uncontrollable; thus, discrepancies from simulated results with actual implementations would likely happen, especially over disconnected and dynamic environments with several types of vehicles.

- **Integrating Encryption into Simulation Tools**

  Another limitation of the simulation in this research is related to the challenges of integrating encryption libraries, such as Crypto++, into simulation tools. While frameworks like OMNeT++ and Veins are very powerful for vehicular network communications, they have not been intrinsically designed to deal with the complexity of cryptographic operations at a large scale. The embedding of some encryption algorithms in the simulated environment raises significant computation overhead and simulation time consumption. Besides, cryptographic processes themselves, such as key management, cycles of encryption/decryption, and certificate validation are rather complex to be simulated realistically.

  In general, several simulations using encryption setups showed that the simulation may or may not truly represent real scenarios where delay in processing or limitation of hardware can make secure communication prohibitive. In this respect, the limitations of the simulation tools regarding the handling of encryption distort the modelled performance from that which may turn out in implementations.

- **Scalability and Real-World Application**

  A scalability limitation is raised under various growth circumstances in communication density and network load perspectives. In the scenarios analysed, a fixed number of vehicles and a specified map size are selected, which makes it challenging to extrapolate the results to larger urban areas or regions with drastically different traffic conditions. With the increase in vehicles, computational overhead for reputation values and certificate management might arise. The pseudonym certificate system works in controlled simulations but may have limitations regarding privacy concerns and real-time processing in more dynamic and densely populated environments.

- **Security and Behavioural Assumptions**

  The final limitation of this study is the assumption of certain malicious behaviours and not delving into such adversarial sophisticated strategies as adaptive attacks, whose characteristics change based on the system's response. Since the conducted study deals with Sybil attacks and incomplete/incorrect data transmission, as relevant as it is, it cannot cover all types of possible attacks aimed at system weaknesses. However, the reputation model assumes that malicious behaviour can be detected and punished based on observable metrics, which could be idealistic in a complex real-world environment whereby adversaries may masquerade as legitimate. For instance, assuming that all vehicles are likely to behave honestly or maliciously over-simplifies a broad spectrum of behaviours possible while on the road.

Given the limitations discussed, the novel reputation schemes proposed in this thesis enable vehicles and reputation server to make more accurate decisions regarding misbehaviours of the receiving messages/reports. Integrating reputation into the existing certification system (SCMS) addresses the verification vulnerabilities and limits misbehaviours in offline scenarios, which traditional systems fail to manage. The research significantly strengthens the trustworthiness of V2V communications during challenging situations.

8.3 Directions for Future Work

While the research introduces a new trust system into vehicular networks that are disconnected, it provides several possibilities for further improvements and extensions. The work can be extended by real-time testing and updating for adaptability to more extensive networks and attack strategies, which will make the proposed scheme more practical and resilient.

- **Real-World Testing**

  The simulation tools adopted in this study provide suitable insight into real-world communications in rural and urban areas. However, further work may be done to deploy the proposed reputation scheme beyond the simulation environment by considering different communication circumstances in order to have a broader view of how the system would behave under varying conditions. This will involve testing with different volumes of traffic, types of vehicles, and environmental factors like weather and infrastructural variabilities. Meanwhile, data from real on-road vehicles that have diversified hardware specifications may improve this system continuously by specifying certain segments that need much more optimization.

- **Real-Time Reputation Update**

  In the proposed reputation system, reputation values are stored and later retrieved from the reputation server upon connectivity. Future work could enhance the reputation scheme's dynamic by updating reputation values based on recent real-time interactions. For example, a vehicle instantly develops a better reputation upon sending a message that gets validated as accurate or trustworthy; another scenario could be that, upon sending false information or acting suspiciously, the reputation goes down instantly. Such continuous adjustment might allow quicker responses to malicious behaviour and cause less additional damage, allowing for faster adaptation to changing network conditions and behaviours, especially in high-mobility scenarios.

- **Adversarial Behaviour and Security Enhancements**

  The study considered Sybil's activity and false reporting attacks in disconnected areas to evaluate the proposed reputation scheme under adversaries. However, further research may develop even more sophisticated adversarial approaches and effective countermeasures for an evolving set of security threats. For instance, further work may consider how adversaries adapt to the reputation-based system by collaboration or other more sophisticated forms of attack, such as evasion or mimicry-based approaches. Implementing dynamic security measures that can evolve alongside these attacks would enhance the system's robustness. Moreover, the inclusion of other metrics of trust, such as behavioural patterns and network trustworthiness, might give a holistic security framework in vehicular networks.

8.4 Enabling Trust in Offline V2V Networks

As the move towards increased automation, connectivity and autonomy of vehicular technology continues, VANETs will play a critical role in improving safety on roads and in enhancing communications. However, the deployment in rural and disconnected areas is extremely challenging. One vital aspect that needs to be enhanced is the V2V decision-making under emergencies, especially in these challenging areas. The research addresses that gap by proposing a reputation-based framework integrated with a pseudonym scheme under the SCMS designed to enable a reliable V2V communications in places with limited infrastructural support.

Trust is important in rural V2V communications, where intermittent connectivity demands decentralised solutions. This work realises trust through the dynamic binding of reputation scores with pseudonym certificates, ensuring privacy for honest vehicles while accurately detecting and penalizing misbehaving entities. The framework balances trust, privacy, and security to improve the reliability of V2V networks even in offline scenarios. The system further enhances the accuracy in misbehaviour detection through robust feedback mechanism that cut down on false reports and make the evaluations credible. Simulations using SUMO, OMNeT++, and Veins show a high accuracy of detection, active isolation of misbehaviour, and preservation of trust in disconnected environments.

This work enables trust in rural V2V communication, filling critical gaps in existing VANET solutions and paving the way for scalable, privacy-preserving, and secure systems. Ultimately, it makes connected and autonomous vehicle technologies inclusive, reliable, and adaptable to underserved regions, promoting safety and the adoption of VANETs.

References

Abbasi, I. A. and Shahid Khan, A. (2018). A review of vehicle to vehicle communication protocols for vanets in the urban environment. *future internet*, 10(2):14.

Abualola, H., Otrok, H., Mizouni, R., and Singh, S. (2022). A v2v charging allocation protocol for electric vehicles in vanet. *Vehicular Communications*, 33:100427.

Agate, V., De Paola, A., Lo Re, G., and Virga, A. (2023). Reputation-based dissemination of trustworthy information in vanets. In *International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services*, pages 445–463. Springer.

Agrawal, S., Tyagi, N., and Misra, A. K. (2016). Seamless vanet connectivity through heterogeneous wireless network on rural highways. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, pages 1–5.

Ahmed, S., Rehman, M. U., Ishtiaq, A., Khan, S., Ali, A., and Begum, S. (2018). Vansec: Attack-resistant vanet security algorithm in terms of trust computation error and normalized routing overhead. *Journal of Sensors*, 2018(1):6576841.

Ahmed, W., Di, W., and Mukathe, D. (2022). A blockchain-enabled incentive trust management with threshold ring signature scheme for traffic event validation in vanets. *Sensors*, 22(17):6715.

Al-shareeda, M. A., Anbar, M., Hasbullah, I. H., Manickam, S., Abdullah, N., and Hamdi, M. M. (2020). Review of prevention schemes for replay attack in vehicular ad hoc networks (vanets). In *2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP)*, pages 394–398. IEEE.

Alalwany, E. and Mahgoub, I. (2024). Security and trust management in the internet of vehicles (iov): Challenges and machine learning solutions. *Sensors*, 24(2):368.

Ali, I., Chen, Y., Ullah, N., Kumar, R., and He, W. (2021). An efficient and provably secure ecc-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in vanets. *IEEE Transactions on Vehicular Technology*, 70(2):1278–1291.

Ali, S., Nand, P., and Tiwari, S. (2022). Detection of wormhole attack in vehicular ad-hoc network over real map using machine learning approach with preventive scheme. *Journal of Information Technology Management*, 14(Special Issue: Security and Resource Management challenges for Internet of Things):159–179.

AlMarshoud, M., Sabir Kiraz, M., and H. Al-Bayatti, A. (2024). Security, privacy, and decentralized trust management in vanets: a review of current research and future directions. *ACM Computing Surveys*, 56(10):1–39.

Amaouche, S., Guezzaz, A., Benkirane, S., Azrour, M., Khattak, S. B. A., Farman, H., and Nasralla, M. M. (2023). Fscb-ids: Feature selection and minority class balancing for attacks detection in vanets. *Applied sciences*, 13(13):7488.

Amari, H., Abou El Houda, Z., Khoukhi, L., and Belguith, L. H. (2023). Trust management in vehicular ad-hoc networks: Extensive survey. *Ieee Access*, 11:47659–47680.

Asghar, M., Doss, R. R. M., and Pan, L. (2018). A scalable and efficient pki based authentication protocol for vanets. In *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–3. IEEE.

Ateniese, G. and Hohenberger, S. (2005). Proxy re-signatures: New definitions, algorithms, and applications. In *Proceedings of the 12th ACM Conference on Computer and Communications Security, ACM*, pages 7–11, Alexandria, VA, USA.

Aurenhammer, F. (1991). Voronoi diagrams—a survey of a fundamental geometric data structure. *ACM Comput. Surv. (CSUR)*, 23:345–405.

Azizi, M. and Shokrollahi, S. (2024). Rtrv: An rsu-assisted trust-based routing protocol for vanets. *Ad Hoc Networks*, 154:103387.

Babaghayou, M., Labraoui, N., Ari, A. A., Lagraa, N., and Ferrag, M. A. (2020). Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey. *Journal of Information Security and Applications*, 55:102618.

Backes, M., Meiser, S., and Schröder, D. (2016). Delegatable functional signatures. In *Public-Key Cryptography—PKC 2016: 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, 6–9 March 2016; Proceedings, Part I*, pages 357–386. Springer, Berlin/Heidelberg, Germany.

Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J., and Park, Y. (2020).

Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. *Ieee Access*, 8:54314–54344.

Banković, Z., Vlajic, M., Puerta, D. S. G., Gonzalez, D. S. S., and Alcaraz, J. (2011). Detecting bad-mouthing attacks on reputation systems using self-organizing maps. *Proceedings of the 4th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2011) held at IWANN 2011*, pages 8–10.

Bao, J., Luo, M., Chen, Y., Peng, C., and Bao, Z. (2024). A certificateless anonymous authentication scheme for vanets based on ring signature. *Journal of Circuits, Systems and Computers*, 33(3):2450053.

Benyamina, Z., Benahmed, K., and Bounaama, F. (2019). Anel: A novel efficient and lightweight authentication scheme for vehicular ad hoc networks. *Computer Networks*, 164:106899.

Bintoro, K. B. Y. (2021). A study of v2v communication on vanet: characteristic, challenges and research trends. *JISA (Jurnal Informatika dan Sains)*, 4(1):46–58.

Brecht, B., Therriault, D., Weimerskirch, A., Whyte, W., Kumar, V., Hehn, T., and Goudy, R. (2018). A security credential management system for v2x communications. *IEEE Trans. Intell. Transp. Syst.*, 19:3850–3871.

Cao, Z., Li, Q., Lim, H. W., and Zhang, J. (2014). A multi-hop reputation announcement scheme for vanets. In *Proceedings of 2014 IEEE International Conference on Service Operations and Logistics, and Informatics*, pages 238–243. IEEE.

Chaouche, Y., Renault, É., and Boussaha, R. (2023). Study of masquerade attack in vanets with machine learning. In *International Conference on Machine Learning for Networking*, pages 167–184. Springer.

Charoenchai, S. and Siripongwutikorn, P. (2024). Genetic algorithm for multi-hop vanet clustering based on coalitional game. *Journal of Network and Systems Management*, 32(1):9.

Chen, A. C., Liu, C.-K., Lin, C.-F., and Lin, B.-Y. (2024). V2x credential management system comparison based on ieee 1609.2. 1 and etsi ts 102 941. In *2024 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, pages 1–6. IEEE.

Cheng, T., Liu, G., Yang, Q., and Sun, J. (2019). Trust assessment in vehicular social network based on three-valued subjective logic. *IEEE Transactions on Multimedia*, 21(3):652–663.

Clancy, J., Mullins, D., Deegan, B., Horgan, J., Ward, E., Eising, C., Denny, P., Jones, E., and Glavin, M. (2024). Wireless access for v2x communications: Research, challenges and opportunities. *IEEE Communications Surveys & Tutorials*.

Cui, B., Wei, L., and He, W. (2022). A new certificateless signcryption scheme for securing internet of vehicles in the 5g era. *Security and Communication Networks*.

Cui, J., Wei, L., Zhang, J., Xu, Y., and Zhong, H. (2018). An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 20(5):1621–1632.

Cui, J., Zhang, J., Zhong, H., and Xu, Y. (2017). Spacf: A secure privacy-preserving authentication scheme for vanet with cuckoo filter. *IEEE transactions on vehicular technology*, 66(11):10283–10295.

Cui, J., Zhang, X., Zhong, H., Zhang, J., and Liu, L. (2019). Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment. *IEEE Trans. Inf. Forensics Secur.*, 15:1654–1667.

Cunha, F., Villas, L., Boukerche, A., Maia, G., Viana, A., Mini, R. A., and Loureiro, A. A. (2016). Data communication in vanets: Protocols, applications and challenges. *Ad hoc networks*, 44:90–103.

Daddanala, R., Mannava, V., Tawlbeh, L., and Al-Ramahi, M. (2021). Vehicle to vehicle (v2v) communication protocol: components, benefits, challenges, safety and machine learning applications. *arXiv preprint arXiv:2102.07306*.

Davis, J. C., Cromartie, J., Farrigan, T., Genetin, B., Sanders, A., and Winikoff, J. B. (2023). Rural america at a glance: 2023 edition. Accessed: 2024-10-16.

Di, C. and Wu, W. (2022). A novel identity-based mutual authentication scheme for vehicle ad hoc networks. *Wireless Communications and Mobile Computing*, 2022(1):7881079.

Douceur, J. R. (2002). The sybil attack. In *International workshop on peer-to-peer systems*, pages 251–260. Springer.

Duan, W., Gu, J., Wen, M., Zhang, G., Ji, Y., and Mumtaz, S. (2020). Emerging technologies for 5g-iov networks: applications, trends and opportunities. *IEEE Network*, 34(5):283–289.

El Sayed, H., Zeadally, S., and Puthal, D. (2020). Design and evaluation of a novel hierarchical trust assessment approach for vehicular networks. *Veh. Commun.*, 24:100227.

ElSalamouny, E., Krukow, K. T., and Sassone, V. (2009). An analysis of the exponential decay principle in probabilistic trust models. *Theoretical computer science*.

Ester, M., Kriegel, H.-P., Sander, J., and Xu, X. (1996). A density-based algorithm for discovering clusters in large spatial databases with noise. In *Proceedings of the 2nd International Conference on Knowledge Discovery and Data Mining (KDD)*, pages 226–231. AAAI Press.

European Telecommunication Standard Institute ETSI40 (2021). TS 102 940; Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management.

European Telecommunication Standard Institute ETSI41 (2021). TS 102 941; Intelligent Transport Systems (ITS); Security; Trust and Privacy Management.

European Telecommunication Standard Institute ETSI72 (2019). EN 302 637-2; Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service.

European Telecommunication Standard Institute ETSI97 (2021). TS 103 097; Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats.

Fujisaki, E. and Suzuki, K. (2007). Traceable ring signature. In *International Workshop on Public Key Cryptography*, pages 181–200. Springer, Berlin/Heidelberg, Germany.

Gaba, S., Gupta, M., and Singh, H. (2023). A comprehensive survey on vanet security attacks. In *AIP Conference Proceedings*, volume 2495. AIP Publishing.

Gao, H., Liu, C., Yin, Y., Xu, Y., and Li, Y. (2021). A hybrid approach to trust node assessment and management for vanets cooperative data communication: Historical interaction perspective. *IEEE Transactions on Intelligent Transportation Systems*, 23(9):16504–16513.

Gao, M., Li, J., Di, X., Li, X., and Zhang, M. (2024). A blind signature scheme for iov based on 2d-scml image encryption and lattice cipher. *Expert Systems with Applications*, 246:123215.

Gayathri, N. B., Thumbur, G., Reddy, P. V., and Rahman, M. Z. U. (2018). Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks. *IEEE Access*, 6:31808–31819.

Ghorai, C. and Banerjee, I. (2018). A constrained delaunay triangulation based rsus deployment strategy to cover a convex region with obstacles for maximizing communications probability between v2i. *Vehicular Communications*, 13:89–103.

Gong, C., Xu, C., Zhou, Z., Zhang, T., and Yang, S. (2019). A reputation management scheme for identifying malicious nodes in vanet. In *2019 IEEE 20th International Conference on High Performance Switching and Routing (HPSR)*, pages 1–6. IEEE.

Google Maps (2025). Map of the peak district, uk. Accessed: 2025-02-25.

Goyal, A. K., Agarwal, G., Tripathi, A. K., and Sharma, G. (2022). Systematic study of vanet: Applications, challenges, threats, attacks, schemes and issues in research. *Green Computing in Network Security*, pages 33–52.

GSMA (2025). Gsma coverage maps. Accessed: 2025-02-27.

Gu, K., Ouyang, X., and Wang, Y. (2024). Malicious vehicle detection scheme based on spatio-temporal features of traffic flow under cloud-fog computing-based iovs. *IEEE Transactions on Intelligent Transportation Systems*.

Guerna, A. and Bitam, S. (2019). Gica: An evolutionary strategy for roadside units deployment in vehicular networks. In *Proceedings of the 2019 International Conference on Networking and Advanced Systems (ICNAS)*, pages 26–27, Annaba, Algeria.

Guerna, A., Bitam, S., and Calafate, C. T. (2022). Roadside unit deployment in internet of vehicles systems: A survey. *Sensors*, 22(9):3190.

Gupta, T., Choudhary, G., and Sharma, V. (2018). A survey on the security of pervasive online social networks (posns). *arXiv preprint arXiv:1806.07526*.

Haas, J. J., Hu, Y.-C., and Laberteaux, K. P. (2011). Efficient certificate revocation list organization and distribution. *IEEE Journal on Selected Areas in Communications*, 29(3):595–604.

Haklay, M. and Weber, P. (2008). Openstreetmap: User-generated street maps. *IEEE Pervasive Computing*, 7(4):12–18.

Hamdi, M. M., Yussen, Y. A., and Mustafa, A. S. (2021). Integrity and authentications for service security in vehicular ad hoc networks (vanets): A review. In *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pages 1–7. IEEE.

Hancock, J., Johnson, J. M., and Khoshgoftaar, T. M. (2022). A comparative approach to threshold optimization for classifying imbalanced data. In *2022 IEEE 8th International Conference on Collaboration and Internet Computing (CIC)*, pages 135–142, Atlanta, GA, USA.

Harshit, G., Akhil, K., Mishra, N., Achyutha, P., and Manitha, P. (2025). V2v communication assisted emergency route optimization. In *2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*, pages 73–78. IEEE.

Hasrouny, H., Samhat, A. E., Bassil, C., and Laouiti, A. (2017). Vanet security challenges and solutions: A survey. *Vehicular Communications*, 7:7–20.

He, D., Zeadally, S., Xu, B., and Huang, X. (2015). An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Transactions on Information Forensics and Security*, 10(12):2681–2691.

Houmer, M. and Hasnaoui, M. L. (2020). A risk and security assessment of vanet availability using attack tree concept. *International Journal of Electrical & Computer Engineering (2088-8708)*, 10(6).

Huo, Y., Yang, R., Jing, G., Wang, X., and Mao, J. (2024). A multi-objective roadside units deployment strategy based on reliable coverage analysis in internet of vehicles. *Ad Hoc Networks*, 164:103630.

Hussain, R., Lee, J., and Zeadally, S. (2020). Trust in vanet: A survey of current solutions and future research opportunities. *IEEE transactions on intelligent transportation systems*, 22(5):2553–2571.

Huynh, T., Jennings, N., and Shadbolt, N. (2006). Certified reputation - how an agent can trust a stranger. In *Proceedings of the 5th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS 2006)*, pages 1217–1224.

IEEE Vehicular Technology Society (2016). IEEE Std 1609.2-2016; IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages.

IEEE Vehicular Technology Society (2022). IEEE Std 1609.2™-2022: IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages.

Jain, E. and Singh, A. (2022). Trust- and reputation-based opinion dynamics modelling over temporal networks. *Journal of Complex Networks*, 10(4):cnac019.

Jansma, N. and Arrendondo, B. (2004). Performance comparison of elliptic curve and rsa digital signatures. *nicj. net/files*.

Jayashree, S. and Kumar, S. S. (2024). An efficient group signature based certificateless verification scheme for vehicular ad-hoc network. *Wireless Networks*, pages 1–30.

Jesús-Azabal, M., Berrocal-Olmeda, J., García-Alonso, J., and Galán-Jiménez, J. (2021). A self-sustainable dtn solution for isolation monitoring in remote areas. In *Gerontechnology III: Contributions to the Third International Workshop on Gerontechnology, IWoG 2020, October 5-6, 2020, Évora, Portugal*, pages 57–68. Springer.

Jiang, S., Chen, X., Cao, Y., Xu, T., He, J., and Cui, Y. (2022). Apki: An anonymous authentication scheme based on pki for vanet. In *2022 7th International Conference on Computer and Communication Systems (ICCCS)*, pages 530–536. IEEE.

Jiang, Y., Ge, S., and Shen, X. (2020). Aaas: An anonymous authentication scheme based on group signature in vanets. *IEEE Access*, 8:98986–98998.

Joharestani, M. Z., Cao, C., Ni, X., Bashir, B., and Talebiesfandarani, S. (2019). Pm$_{2.5}$ prediction based on random forest, xgboost, and deep learning using multisource remote sensing data. *Atmosphere*, 10(7):373.

Jøsang, A. (2006). Trust and reputation systems. In *International School on Foundations of Security Analysis and Design*, pages 209–245. Springer.

Joshi, A., Gaonkar, P., and Bapat, J. (2017). A reliable and secure approach for efficient car-to-car communication in intelligent transportation systems. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pages 1617–1620. IEEE.

Kabbur, M. and Murthy, M. (2023). Mvr delay: Cooperative light weight detection and prevention of false emergency message dissemination in vanet. In *Proceedings of the International Conference on Cognitive Computing and Information Processing*, pages 25–38, Cham. Springer Nature Switzerland.

Kahn, C. A. (2015). National highway traffic safety administration (nhtsa) notes. *Ann. Emerg. Med.*, 66:669–669.

Kamel, J., Ansari, M. R., Petit, J., Kaiser, A., Jemaa, I. B., and Urien, P. (2020). Simulation framework for misbehavior detection in vehicular networks. *IEEE transactions on vehicular technology*, 69(6):6631–6643.

Karabulut, M. A., Shah, A. S., Ilhan, H., Pathan, A.-S. K., and Atiquzzaman, M. (2023). Inspecting vanet with various critical aspects–a systematic review. *Ad Hoc Networks*, page 103281.

Katiyar, A., Gupta, S. K., Singh, D., and Yadav, R. S. (2020). A dynamic single-hop clustering algorithm (dsca) in vanet. In *2020 11th international conference on computing, communication and networking technologies (ICCCNT)*, pages 1–6. IEEE.

Ke, C., Xiao, F., Cao, Y., and Huang, Z. (2024). A group-vehicles oriented reputation assessment scheme for edge vanets. *IEEE Transactions on Cloud Computing*.

Kenney, J. B. (2011). Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182.

Kerrache, C. A., Lakas, A., and Lagraa, N. (2016). Detection of intelligent malicious and selfish nodes in vanet using threshold adaptive control. In *2016 5th international conference on electronic devices, systems and applications (ICEDSA)*, pages 1–4. IEEE.

Khan, A. R., Jamlos, M. F., Osman, N., Ishak, M. I., Dzaharudin, F., Yeow, Y. K., and Khairi, K. A. (2022). Dsrc technology in vehicle-to-vehicle (v2v) and vehicle-to-infrastructure (v2i) iot system for intelligent transportation system (its): A review. *Recent Trends in Mechatronics Towards Industry 4.0: Selected Articles from iM3F 2020, Malaysia*, pages 97–106.

Khan, S., Zhu, L., Yu, X., Zhang, Z., Rahim, M., Khan, M., Du, X., and Guizani, M. (2020). Accountable credential management system for vehicular communication. *Veh. Commun.*, 25:100279.

Kosmopoulos, I., Skondras, E., Michalas, A., Michailidis, E. T., and Vergados, D. D. (2022). Handover management in 5g vehicular networks. *Future Internet*, 14(3).

Koukis, G., Safouri, K., and Tsaoussidis, V. (2024). All about delay-tolerant networking (dtn) contributions to future internet. *Future Internet*, 16(4):129.

Krawczyk, H., Paterson, K. G., and Wee, H. (2013). On the security of the tls protocol: A systematic analysis. In *Annual Cryptology Conference*, pages 429–448. Springer.

Kumar, P., Kumari, S., Sharma, V., Li, X., Sangaiah, A. K., and Islam, S. K. H. (2019). Secure cls and cl-as schemes designed for vanets. *Journal of Supercomputing*, 75:3076–3098.

Kuntke, F. (2024). Rural communication in outage scenarios: Disruption-tolerant networking via lorawan setups. In *Resilient Smart Farming: Crisis-Capable Information and Communication Technologies for Agriculture*, pages 205–224. Springer.

Li, Q., Malip, A., Martin, K., Ng, S., and Zhang, J. (2012). A reputation-based announcement scheme for vanets. *IEEE Trans. Veh. Technol.*, 61:4095–4108.

Li, X., Han, Y., Gao, J., and Niu, J. (2020). Secure hierarchical authentication protocol in vanet. *IET Information Security*, 14(1):99–110.

Li, X. and Yin, X. (2022). Blockchain-based group key agreement protocol for vehicular ad hoc networks. *Computer Communications*, 183:107–120.

Liang, B., Wang, F., and Ran, B. (2024). Optimizing roadside unit deployment in vanets: A study on consideration of failure. *IEEE Transactions on Intelligent Transportation Systems*.

Liu, Y., Guo, W., Zhong, Q., and Yao, G. (2017). Lvap: Lightweight v2i authentication protocol using group communication in vanet s. *International Journal of Communication Systems*, 30(16):e3317.

Liu, Z.-C., Xiong, L., Peng, T., Peng, D.-Y., and Liang, H.-B. (2018). A realistic distributed conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Access*, 6:26307–26317.

Lopez, P., Behrisch, M., Bieker-Walz, L., Erdmann, J., Flötteröd, Y.-P., Hilbrich, R., Lücken, L., Rummel, J., Wagner, P., and Wießner, E. (2018). Microscopic traffic simulation using sumo. In *21st IEEE International Conference on Intelligent Transportation Systems, IEEE Intelligent Transportation Systems Conference (ITSC)*, pages 4–7, Maui, HI, USA.

Lui, G. L. (1998). Threshold detection performance of gmsk signal with bt=0.5. In *IEEE Military Communications Conference. Proceedings. MILCOM 98 (Cat. No.98CH36201)*, pages 515–519 vol.2, Boston, MA, USA.

Lv, P., Xie, L., Xu, J., Wu, X., and Li, T. (2022). Misbehaviour detection in vehicular ad hoc networks based on privacy-preserving federated learning and blockchain. *IEEE Transactions on Network and Service Management*, 19(4):3936–3948.

Mahesh, R. and Jawaligi, S. S. (2024). Vanet cluster-based routing protocol with link breakage handling: introduction to hybrid optimization algorithm. *Signal, Image and Video Processing*, pages 1–10.

Makkawi, A., Daher, R., and Rizk, R. (2015). Rsus placement using cumulative weight based method for urban and rural roads. In *2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM)*, pages 307–313. IEEE.

Mariani, R. (2018). An overview of autonomous vehicles safety. In *2018 IEEE International Reliability Physics Symposium (IRPS)*, pages 6A–1. IEEE.

Marzouk, F., Alheiro, R., Rodriguez, J., and Radwan, A. (2018). Enhanced reachability and low latency denm dissemination protocol for platoon based vanets. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–7. IEEE.

Mistareehi, H. (2021). Message dissemination scheme for rural areas using vanet (hardware implementation). In *2021 Twelfth International Conference on Ubiquitous and Future Networks (ICUFN)*, pages 120–125. IEEE.

Mittal, Y. R. (2024). *A simulation study to analyse the impact of V2X communication on the emergency vehicle response time*. PhD thesis, Technische Hochschule Ingolstadt.

Morra, L., Lamberti, F., Pratticó, F. G., La Rosa, S., and Montuschi, P. (2019). Building trust in autonomous vehicles: Role of virtual reality driving simulators in hmi design. *IEEE Transactions on Vehicular Technology*, 68(10):9438–9450.

Mosadegh, H. and Farzaneh, N. (2021). Scds: A secure clustering protocol using dempster-shafer theory for vanet in smart city. In *2021 11th International Conference on Computer Engineering and Knowledge (ICCKE)*, pages 13–18. IEEE.

Mutzenich, C., Durant, S., Helman, S., and Dalton, P. (2021). Situation awareness in remote operators of autonomous vehicles: Developing a taxonomy of situation awareness in video-relays of driving scenes. *Frontiers in psychology*, 12:727500.

Nath, H. J. and Choudhury, H. (2022). A privacy-preserving mutual authentication scheme for group communication in vanet. *Computer Communications*, 192:357–372.

Nathi, N. G. (2024). Misbehaviour detection in vehicular networks using unsupervised algorithms. Master's thesis, University of Windsor, Canada.

National Research Council US, C. f. R. o. t. U. D. o. T. I. T. S. S. P. (2000). Standards for intelligent transportation systems: Review of the federal program. (Special Report 267).

Nawaz, A. and Sattar, A. (2016). Traffic analysis in rural/urban area using vanet routing protocols. adv automob eng s1: 004. doi: 10.4172/2167-7670. s1-00 4 page 2 of 5 adv automob engg issn: 2167-7670 aae, an open access journal hybrid electrical. *Fuel Cell Vehicles The WAVE stack uses IEEE802*.

Nguyen, V.-L., Lin, P.-C., and Hwang, R.-H. (2020). Enhancing misbehavior detection in 5g vehicle-to-vehicle communications. *IEEE Transactions on Vehicular Technology*, 69(9):9417–9430.

Pandey, P. K., Kansal, V., and Swaroop, A. (2023). Security challenges and solutions for next-generation vanets: an exploratory study. In *Role of Data-Intensive Distributed Computing Systems in Designing Data Solutions*, pages 183–201. Springer.

Papadimitratos, P. (2024). Secure vehicular communication systems. In *Encyclopedia of Cryptography, Security and Privacy*, pages 1–6. Springer, Berlin, Heidelberg.

Patel, P., Sharma, R., and SVITS, I. (2015). Rural and urban area based distribution routing using proactive and reactive routing protocol in vanet. *International Journal of Technology Research and Management*, 2(4).

Pathrose, P. (2024). *ADAS and Automated Driving: Systems Engineering*. SAE International.

Patil, P. and Gokhale, A. (2013). Voronoi-based placement of road-side units to improve dynamic resource management in vehicular ad hoc networks. In *Proceedings of the 2013 International Conference on Collaboration Technologies and Systems (CTS)*, pages 20–24, San Diego, CA, USA.

Perumal, S., Raman, V., Samy, G. N., Shanmugam, B., Kisenasamy, K., and Ponnan, S. (2022). Comprehensive literature review on delay tolerant network (dtn) framework for improving the efficiency of internet connection in rural regions of malaysia. *International Journal of System Assurance Engineering and Management*, 13(Suppl 1):764–777.

Pointcheval, D. and Stern, J. (2000). Security arguments for digital signatures and blind signatures. *J. Cryptol.*, 13:361–396.

Pooja, B., Pai, M. M., Pai, R. M., Ajam, N., and Mouzna, J. (2014). Mitigation of insider and outsider dos attack against signature based authentication in vanets. In *2014 Asia-Pacific Conference on Computer Aided System Engineering (APCASE)*, pages 152–157. IEEE.

Qi, J. and Gao, T. (2020). A privacy-preserving authentication and pseudonym revocation scheme for vanets. *IEEE Access*, 8:177693–177707.

Raghu, R., Jayanatiya, J., Karunya, A., Meena, M., and Rakshana, A. (2020). A trust scheme based on event report for communication in vanets (tserc). *academia. edu,[Online]. Available: https://www. academia. edu/download/67395826/IJARCCE.*

Raghuwanshi, V. and Jain, S. (2015). Denial of service attack in vanet: a survey. *International Journal of Engineering Trends and Technology (IJETT)*, 28(1):15–20.

Ramraj, S., Uzir, N., Sunil, R., and Banerjee, S. (2016). Experimenting xgboost algorithm for prediction and classification of different datasets. *International Journal of Control Theory and Applications*, 9(40):651–662.

Rescorla, E. (2018). The transport layer security (tls) protocol version 1.3. Technical Report RFC 8446, Internet Engineering Task Force.

Ripan, R. C., Sarker, I. H., Anwar, M. M., Furhad, M. H., Rahat, F., Hoque, M. M., and Sarfraz, M. (2021). An isolation forest learning based outlier detection approach for effectively classifying cyber anomalies. In *Hybrid Intelligent Systems: 20th International Conference on Hybrid Intelligent Systems (HIS 2020)*, pages 270–279. Springer International Publishing.

SAE International (2020). SAE J2735: Dedicated Short Range Communications (DSRC) Message Set Dictionary. Accessed: 2024-08-10.

SAE International (2021). Sae levels of driving automation™ refined for clarity and international audience. Accessed: 2024-08-10.

Samara, G. (2020). Intelligent reputation system for safety messages in vanet. *arXiv preprint arXiv:2007.12717.*

Samara, G. and Alsalihy, W. (2012). A new security mechanism for vehicular communication networks. In *Proceedings of the 2012 International*

Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec 2012).

Scalise, P., Boeding, M., Hempel, M., Sharif, H., Delloiacovo, J., and Reed, J. (2024). A systematic survey on 5g and 6g security considerations, challenges, trends, and research areas. *Future Internet*, 16(3):67.

Shahabi, H. G. and Soni, S. (2023). Security and privacy challenges in vehicular ad-hoc networks: Threats, countermeasures. *Eigenpub Review of Science and Technology*, 7(1):22–38.

Shaikh, R. A. and Alzahrani, A. S. (2013). Trust management method for vehicular ad hoc networks. In *Quality, Reliability, Security and Robustness in Heterogeneous Networks: 9th International Conference, QShine 2013, Greader Noida, India, January 11-12, 2013, Revised Selected Papers 9*, pages 801–815. Springer.

Shurrab, M., Singh, S., Otrok, H., Mizouni, R., Khadkikar, V., and Zeineldin, H. (2021). An efficient vehicle-to-vehicle (v2v) energy sharing framework. *IEEE Internet Things J.*, 9:5315–5328.

Simplicio, M., Cominetti, E., Patil, H., Ricardini, J., and Silva, M. (2018). The unified butterfly effect: Efficient security credential management system for vehicular communications. In *Proceedings of the 2018 IEEE Vehicular Networking Conference (VNC)*, pages 5–7, Taipei, Taiwan.

Sirur, S. and Muller, T. (2019). The reputation lag attack. In *Trust Management XIII: 13th IFIP WG 11.11 International Conference, IFIPTM 2019, Copenhagen, Denmark, July 17-19, 2019, Proceedings 13*, pages 39–56. Springer.

Soleymani, S. A., Goudarzi, S., Anisi, M. H., Zareei, M., Abdullah, A. H., and Kama, N. (2021). A security and privacy scheme based on node and message authentication and trust in fog-enabled vanet. *Vehicular Communications*, 29:100335.

Sommer, C., German, R., and Dressler, F. (2011). Bidirectionally coupled network and road traffic simulation for improved ivc analysis. *IEEE Trans. Mob. Comput.*, 10:3–15.

Tahir, M. N., Leviäkangas, P., and Katz, M. (2022). Connected vehicles: V2v and v2i road weather and traffic communication using cellular technologies. *Sensors*, 22(3):1142.

Tan, H., Gui, Z., and Chung, I. (2018). A secure and efficient certificateless authentication scheme with unsupervised anomaly detection in vanets. *IEEE Access*, 6:74260–74276.

Tao, R., Wolleschensky, L., and Weimerskirch, A. (2019). Security certificate management system for v2v communication in china. *SAE Int. J. Transp. Cyber. Privacy*, 2:169–183.

Tian, J., Wang, Y., and Shen, Y. (2024). An identity-based authentication scheme with full anonymity and unlinkability for mobile edge computing. *IEEE Internet of Things Journal*, 2024.

Tian, Z., Gao, X., Su, S., and Qiu, J. (2019). Vcash: a novel reputation framework for identifying denial of traffic service in internet of connected vehicles. *IEEE Internet of Things Journal*, 7(5):3901–3909.

Tiwari, S. D., Hota, L., Nayak, B. P., and Kumar, A. (2024). Beyond trust: Leveraging blockchain for privacy-centric vanet authentication. In *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, pages 1–7. IEEE.

Townsend, J. T. (1971). Theoretical analysis of an alphabetic confusion matrix. *Perception & Psychophysics*, 9:40–50.

Ullah, S., Abbas, G., Waqas, M., Abbas, Z. H., and Khan, A. U. (2023). Rsu assisted reliable relay selection for emergency message routing in intermittently connected vanets. *Wireless Networks*, 29(3):1311–1332.

U.S. Department of Transportation, National Highway Traffic Safety Administration (2018). U.S. DOT Federal Motor Vehicle Safety Standards; V2V Communications; NPRM.

Vaiana, R., Perri, G., Iuele, T., and Gallelli, V. (2021). A comprehensive approach combining regulatory procedures and accident data analysis for road safety management based on the european directive 2019/1936/ec. *Safety*, 7(1):6.

Vamshi Krishna, K. and Ganesh Reddy, K. (2023). Classification of distributed denial of service attacks in vanet: a survey. *Wireless Personal Communications*, 132(2):933–964.

Van Der Heijden, R. W., Dietzel, S., Leinmüller, T., and Kargl, F. (2018). Survey on misbehavior detection in cooperative intelligent transportation systems. *IEEE Communications Surveys & Tutorials*, 21(1):779–811.

van Eenennaam, M., van de Venis, A., and Karagiannis, G. (2012). Impact of ieee 1609.4 channel switching on the ieee 802.11p beaconing performance. In *2012 IFIP Wireless Days*, pages 1–8.

Vinita, L. J. and Vetriselvi, V. (2023). Federated learning-based misbehaviour detection on an emergency message dissemination scenario for the 6g-enabled internet of vehicles. *Ad Hoc Networks*, 144:103153.

Wan, H., Wang, H., Scotney, B., and Liu, J. (2019). A novel gaussian mixture model for classification. In *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, pages 3298–3303. IEEE.

Wang, S. and Yao, N. (2019). A rsu-aided distributed trust framework for pseudonym-enabled privacy preservation in vanets. *Wireless Networks*, 25:1099–1115.

Wen, H., Huang, P. Y.-R., Dyer, J., Archinal, A., and Fagan, J. (2005). Countermeasures for gps signal spoofing. In *Proceedings of the 18th international technical meeting of the satellite division of the institute of navigation (ION GNSS 2005)*, pages 1285–1290.

Whyte, W., Weimerskirch, A., Kumar, V., and Hehn, T. (2013). A security credential management system for v2v communications. In *2013 IEEE Vehicular Networking Conference*, pages 1–8. IEEE.

World Bank (2024). World bank annual report 2024. License: CC BY-NC-ND 3.0 IGO.

Wu, C.-M., Tsai, C.-T., Hou, C.-C., Yang, J.-J., Lin, G.-D., and Kuang, M.-Y. (2024). Emergency message broadcast mechanism in vehicular ad-hoc networks based on reinforcement learning with contention estimation. *IEEE Transactions on Intelligent Vehicles*.

Xie, Q., Ding, Z., and Zheng, P. (2023). Provably secure and anonymous v2i and v2v authentication protocol for vanets. *IEEE Trans. Intell. Transp. Syst.*, 24:7318–7327.

Xiong, X., Xu, W., and Zhao, G. (2018). The effectiveness assessment for network based mtd strategies. In *Proceedings of the 8th International Conference on Communication and Network Security*, pages 7–11.

Xu, X., Wang, Y., Qin, H., Zhang, J., Yan, M., and Ji, H. (2020). Secured authentication method in v2x communication scenario. In *CICTP 2020*. CICTP.

Yang, J., Liang, N., Pitts, B. J., Prakah-Asante, K. O., Curry, R., Blommer, M., Swaminathan, R., and Yu, D. (2023). Multimodal sensing and computational intelligence for situation awareness classification in autonomous driving. *IEEE Transactions on Human-Machine Systems*, 53(2):270–281.

Yogarayan, S., Razak, S. F. A., Azman, A., Abdullah, M. F. A., Ibrahim, S. Z., and Raman, K. J. (2020). A review of routing protocols for vehicular ad-hoc networks (vanets). In *2020 8th International Conference on Information and Communication Technology (ICoICT)*, pages 1–7. IEEE.

Yousaf, I. and Majeed, N. (2017). Comparative analysis and performance evaluation of olsr, aodv, grp for urban and ruralareas in vanets. *NFC IEFR Journal of Engineering and Scientific Research*, 3.

Yu, H., Liu, R., Li, Z., Ren, Y., and Jiang, H. (2022). An rsu deployment strategy based on traffic demand in vehicular ad hoc networks (vanets). *IEEE Internet Things J.*, 9:6496–6505.

Zeddini, B., Maachaoui, M., and Inedjaren, Y. (2022). Security threats in intelligent transportation systems and their risk levels. *Risks*, 10:91.

Zhang, B., Huang, Z., and Xiang, Y. (2014). A novel multiple-level trust management framework for wireless sensor networks. *Computer Networks*, 72:45–61.

Zhang, J. and Hu, G. (2024). Road side unit deployment optimization for the reliability of internet of vehicles based on information transmission model. *PloS one*, 19(12):e0315716.

Zhang, J., Zhang, Q., Lu, X., and Gan, Y. (2021). A novel privacy-preserving authentication protocol using bilinear pairings for the vanet environment. *Wireless Communications and Mobile Computing*, 2021(1):6692568.

Zhang, L., Wang, L., Zhang, L., Zhang, X., and Sun, D. (2023). An rsu deployment scheme for vehicle-infrastructure cooperated autonomous driving. *Sustainability*, 15(4):3847.

Zhang, S., Liu, Y., Xiao, Y., and He, R. (2022). A trust based adaptive privacy preserving authentication scheme for vanets. *Vehicular Communications*, 37:100516.

Zhou, Y., Wang, Z., Qiao, Z., Yang, B., and Zhang, M. (2023). An efficient and provably secure identity authentication scheme for vanet. *IEEE Internet of Things Journal*, 10(19):17170–17183.

Zhu, X., Hu, D., Hou, Z., and Ding, L. (2014). A location privacy preserving solution to resist passive and active attacks in vanet. *China Communications*, 11(9):60–67.

Appendices

Appendix A

Preliminary Simulation Study

Reputation Mechanism Simulations for V2V Communication in Limited Infrastructure Scenarios

Dimah Almani, Steven Furnell, and Tim Muller
School of Computer Science, University of Nottingham, United Kingdom

Abstract

Vehicle to Vehicle (V2V) networking is a promising technology that ensures secure and efficient transportation by allowing vehicles to communicate and share messages to alert each other.In such a network, reputation can be used to establish trust between vehicles in disconnected areas. While a vehicle with a low reputation could be less trustworthy, a vehicle with a high reputation is supposed to be more reliable. This concept can be implemented if every vehicle is given a reputation score. Reputation score can be determined by a reputation server linked to a Security Credential Management System, which uses data from onboard sensors or past interactions with other vehicles. In this work, we incorporate a reputation system to maximize the chance of making an accurate decision based on the received message. By adopting the pre-signature scheme, vehicles dynamically assess and rely on the most trustworthy information available, even in the most challenging and infrastructure-limited environment. The simulation shows the effectiveness achieved by our proposed schema using reputation values to improve the safety and efficiency of offline V2V communication by preventing accidents and attacks and reducing traffic congestion.

1. Introduction

In vehicle-to-vehicle (V2V) communication, vehicles share information like location, driving behavior, and road conditions to improve safety and efficiency on the road. In rural areas, the connectivity is limited. To illustrate, while GSM communications technologies are certainly widespread, they are not universally accessible, due to geographic limitations. For example, from GSMA website, it is clear that the coverage in the some areas is not always guaranteed, and it is easy to find many areas in different countries where there is road infrastructure but a lack of 2G coverage. In such a condition, vehicles solely rely on neighbouring vehicles for communication, necessitating trust and reliability among them. Existing authentication systems such as Security Credential Management System (SCMS) supply the vehicles with certificates to meet the security and privacy requirements [1]. However, this system has difficulty ensuring that invalid certificates are up to date in areas with limited internet access. Reputation, which reflects a vehicle's trustworthiness based on past behavior, is an important measure of the accuracy and reliability of the information transmitted. A vehicle's reputation can be influenced by factors like compliance with communication protocols, accuracy of information, and overall behavior on the road. Reputation-based systems can be used in rural scenarios to assess the trustworthiness of other vehicles and determine which ones are most reliable. Vehicles with higher Reputation Value (RV) are more likely to be trusted, while those with lower scores are less likely to be trusted. These systems can also be used to identify malicious behavior or cyber-attacks, where a vehicle found to be spreading false or harmful information has its RV lowered.

In this work, we implement a reputation mechanism as a verification tool in rural areas. When a vehicle receives a message from another vehicle, it checks the sender's RV against a pre-defined acceptance threshold or criteria. We employ simulation setup for real-time communications. The simulation integrates the capabilities of the Urban Mobility Simulation (SUMO), Objective Modular Network Testbed in C++ (OMNeT++), and Vehicles in Network Simulation (Veins). This integrated simulation environment allows for the realistic modeling of vehicular movements, network communications, and the complex interplay between vehicles exchanging emergency messages within the DSRC effective range of 1000 meters. Through the simulation experiments, we demonstrate how our reputation-based approach, supported by the *Pre-Signature* authentication mechanism, as explained in [2, 3] significantly enhances the decision accuracy in V2V communications under the constrained conditions characteristic of rural environments. In the following, Section 2 discusses the related work, and Section 3 introduces the reputation system. Section 4 describes the simulation work and the proposed mechanism. Section 5 discusses the simulation results. Section 6 concludes our work highlighting the key findings in this study.

2. Related Work

Reputation has been an active research field for the last decades and many reputation systems in the Vehicular networks including decision making have been discussed leading to the proposal of various studies that aim to limit the consequences of having conflicting reports in emergency scenarios. However, it is worth noting that the issue of conflicting messages within a limited infrastructure areas has remained relatively unexplored in existing studies.

A reputation system for VANETs was first introduced by Li et al [4]; based on a centralized reputation scheme that centrally disseminates, update, and store vehicles' RVs. A reputation announcement scheme based on Time Threshold was designed to evaluate message reliability. El et al. [5], and Naskath et al. [6] designed a node reputation mechanism to evaluate the reliability of both vehicles and their messages: Vehicles that are close to each other and have the same mobility patterns are grouped into a platoon to reduce propagation overhead. Kudva et al [7] suggested a framework of self-organized vehicles to filter the malicious vehicles based on the standard score. Reputation-based mechanism proposed by Agate et al. [8], evaluates the credibility of accident reports in V2V communication systems by considering a vehicle's reporting history, their reputation system improves accident detection accuracy. However, previous work primarily focuses on reputation alone, without fully incorporating other relevant factors. Security Credential Management System (SCMS) needs to be considered in the research as a PKI-base infrastructure that provides a secure authentication, authorization, and data integrity for V2V communication [9], [10].

In SCMS, a Certificate Revocation List (CRL) is maintained to identify and block misbehaving vehicles from the communication network assisting the vehicles to avoid untrusted or malicious vehicles. However, the CRL must be synchronised when vehicles have access to the infrastructure, e.g. via Road side Units (RSUs) [11] and accessing the updated CRLs is challenging in rural area with limited infrastructure, Hence, we propose a mechanism that is more scalable than a CRL, and uses a more granular notion of reputation

In summary, earlier works have focused on reputation mechanisms, proximity analysis, severity assessment, and security in V2V communication. Our contribution is a simulation-based solution that integrates these factors with the reputation for precise and reliable conflict resolution in challenging scenarios.

3. Reputation System

In this section, we discuss the main assumptions following by the receiving message protocols used in this work.

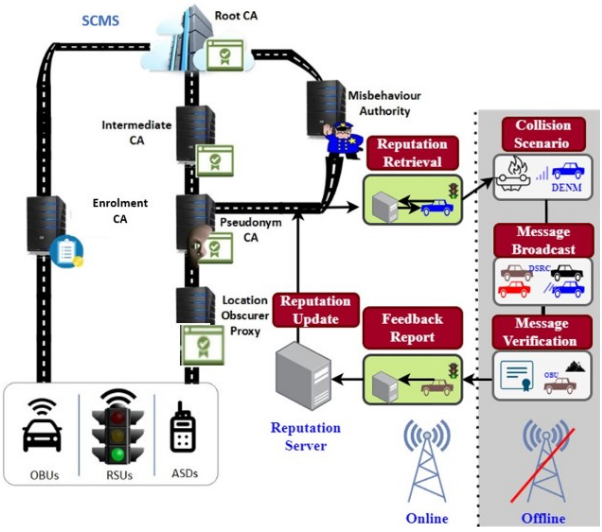


Figure 1. Proposed system model

3.1. System Assumptions

As shown in Figure1, the Reputation Server (RS) is linked to the SCMS to ensure that only authorized vehicles can participate in communications. This involves establishing a secure and trusted credential management system to authenticate vehicles. A vehicle with valid certificates and a high reputation is more credible than a vehicle with invalid certificates and a low reputation. The system is based on the pre-signature scheme as explained in [2, 3], designed in a destabilized manner to operate in low-infrastructure environments.

In this system, we consider both positive and negative interactions between vehicles that are classified into honest nodes that behave normally and forward the message without any changes and malicious nodes that change the contents of the received message to disrupt communication.

Vehicles should be willing to share information and alert other vehicles during emergencies which is a necessary step of the RV computation, as the reputation of each vehicle is based on feedback from other vehicles. Using reputation-based Pseudonym Certificates (PCs) requires encryption and security mechanisms to protect sensitive information against unauthorized access resulting in the preservation of the privacy of vehicles within the network to prevent the leakage of personal information.

3.2. Receiving Emergency Messages

This section explains a scenario and a process for verifying and authenticating messages received by a vehicle from another vehicle in offline sitting. The process involves several checks, including verifying the reputation of the sending vehicle and the validity of the message's signature, timestamp, and proof of reputation.

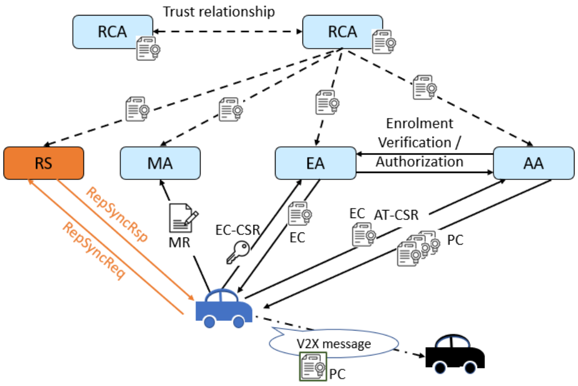


Figure 2. SCMS architecture with RS.

The given scenario, Figure 2, describes an experiment in which two vehicles (V1 and V2) are equipped with Dedicated Short Range Communication (DSRC) modules to communicate with each other while moving along a road in the same direction. The procedure to verify the receiving message as follows:

1. Each vehicle maintains RVs for all the other vehicles it has exchanged data in the past. The RV is updated based on the feedback provided by other vehicles to the RS.

2. The receiving vehicle first verifies the PC attached to the message to check the sender's eligibility. If the eligibility of the sender is verified, the recipient vehicle checks the sender's RV to assess whether it is reputable.

3. If the sender's RV is verified and it is above the threshold of 0.5, then the message is considered to be reliable and can be taken into consideration. Otherwise, it is discarded.

4. If the sender is not reputable, the receiving vehicle can still choose to accept the message if it has been signed by SCMS. In this case, the receiving vehicle would verify the signature to ensure that the message has not been tampered with.

5. The receiving vehicle stores the message, the PC, RV of the sending vehicle for future feedback reporting.

In this procedure, the PC is used to verify the eligibility of the sending vehicle before the RV is checked. This ensures that the receiving vehicle is communicating with the correct vehicle and can therefore rely on its RV. The PC is also included with the message and stored for future feedback reporting. Additionally, the periodic broadcast of both the reputation score and the PC helps to ensure that both are kept up-to-date and accurate.

4. Simulation Environment Setting

This section discusses the simulation scenario, focusing on rural areas with limited infrastructure. It introduces the simulation's core concept and explains the design of the main scenario and the setup of the experiments.

4.1. Simulation Concept Overview

This simulation focuses on V2V communication in the Peak District, a National Park in central England aiming to measure the impact of reputation during emergencies in a rural area with limited infrastructure. Over a 24-hour period, the simulation replicates real-world driving conditions to evaluate connectivity challenges due to sparse connectivity coverage. We investigate scenarios where vehicles are frequently out of infrastructure range, and rely on direct communication so to alert each other about an accident. This simulation is used to demonstrate the effectiveness of the proposed Pre-signature scheme [3], since it enables vehicles to authenticate and validate messages for proper decision-making during such an emergency situation.

4.2. Scenario Design

This section elaborates on the specific accident scenarios carefully crafted for our simulations. Using the simulators with an upper layer routing protocol, the simulation lasted 2100 seconds, featuring an accident at 40 seconds and an attack at 70 seconds. This scenario occurs in a disconnected area with a total of 200 vehicles are communicating under a limited connectivity coverage. One vehicle suddenly loses control and crashes, blocking the road and creating a hazardous situation for other drivers. During the accident, the vehicle periodically communicates with other nearby vehicles using the DSRC. It broadcasts beacon packets as emergency messages to all the vehicles within its range, alerting them about the accident and advising them to change the direction. These messages contain information about the location of the accident, the type of incident, and any other relevant details. The RV will be attached with each message using the Pre-signature scheme. Based on these reputation values, the receiving vehicles in the vicinity receive the message, verify the PC and RV then make the desion (accept/reject). Some may choose to slow down or stop altogether to avoid getting involved in the accident, while others may take alternative routes to reach their destination. However, in this scenario, the risk that some of the vehicles receiving the emergency message may be untrusted or malicious has been tested. For example, a malicious vehicle may try to manipulate the message to mislead other drivers and cause further chaos on the road.

4.3. Experimental Setup

The simulation conducted using OMNeT++, Veins, and SUMO to validate the proposed model utilizing IEEE 802.11p/1609.4 protocols. To facilitate this simulation, the Trace Control Interface *TraCI* acted as an intermediary between OMNeT++ and SUMO++, establishing TCP-based communication between these two simulators. The communication modules use DSRC with 5.9 GHz spectrum band and have 7 channels available, of which 1 is a control channel for broadcasting security messages and the remaining 6 channels are used for V2V communication. Each channel has a bandwidth of 10 MHz, and the data transfer rate can be up to 27 Mbps, which means that each vehicle can transmit and receive data at a maximum speed of 27 megabits per second. We generated all the needed compounds to set up and run this new scenario. This scenario includes an accident event and the attack scenario. To assess the model's performance, specific parameters were selected, as outlined in Table 1.

Table 1. Simulation parameters

Parameter	**Value**
Network size (km)	3*3
Mobility model	Peak District
Vehicle communication standard	(DSRC) IEEE 802.11 P
Transmission Range: R(Mm)	250
Simulation Time	2100s
Number of vehicles per kilometer:	10, 15, 20,25,30, 50
Data Transmission rate(Mbps)	27
Emergency packet size (bytes)	514
Emergency packet generation intervals (s)	0.05, 01, 05, 1
Minimum transmission frequency (Hz)	10
Required latency (ms)	< 100
Road side Unites (RSU)	No
Number of Accident	1
Accident Duration	60s
Vehicle Length	2.5
Road Type	Multiple-ways

In the testing scenario, we first implemented the Omnetpp.ini as the basic file to run the simulation. It contains all the needed parameters to set up the scenario. Then, we designed the NED file which is necessary to describe the used compound (implementation classes) and their default configuration. After this, we implemented the XML files for SUMO configuration. Those files describe: the obstacle model, propagation model(config.xml), the antenna model (antenna.xml), and configuration file to run the Sumo.gui. We then included the Sumo launching files such as rou and poly files that describe the driving scenario, the topology and the routes in the used map. In addition, we designed the reputationScoreFile that contains the following elements for each node in the network: The node id which is a unique identifier used in the simulation scenario; the Reputation scores ranging from 0 to 1; and the Malicious state, we set it as 0 for legitimate node and 1 for a malicious node.

4.4. Experiment Process

As shown in Figure 3, we implement our reputation scheme to verify the messages in rural areas ensures the following functionalities:

- Monitor the position update: this functionality supervises the vehicle's position and detects any LONG STOP caused by an accident. When an accident happens, an alert message is broadcast to inform vehicles in the same network.
- Handle ALERT message: This feature defines the action taken by a vehicle when it receives an alert message. Each vehicle requests a route change to avoid a road accident.
- Manage the reputation score: This feature handles the use of the reputation score.
  - Each node gets its own score.
  - Each node stores the score of all other nodes in the network.
  - Each node introduces its identifier in any ALERT message sent, so receiving nodes read this identifier and are able to verify the state of each node (Legitimate or malicious node)
- Manage the malicious action: Each node set as attacker (malicious node) is able to send a FALSE ALERT. This alert contains false information (false accident, false accident road, false time, etc..…)

Receiving the ALERT message: This is done by the method onWSM(), which is called when the node receives the ALERT message. First the node extracts the node Identifier from the message. Then, it verifies if the score of the sender is greater than the defined Threshold. Two cases are possible: 1-The sender score is lower. So the node is untrusted vehicle. The receiver drops the ALERT message. 2-The sender

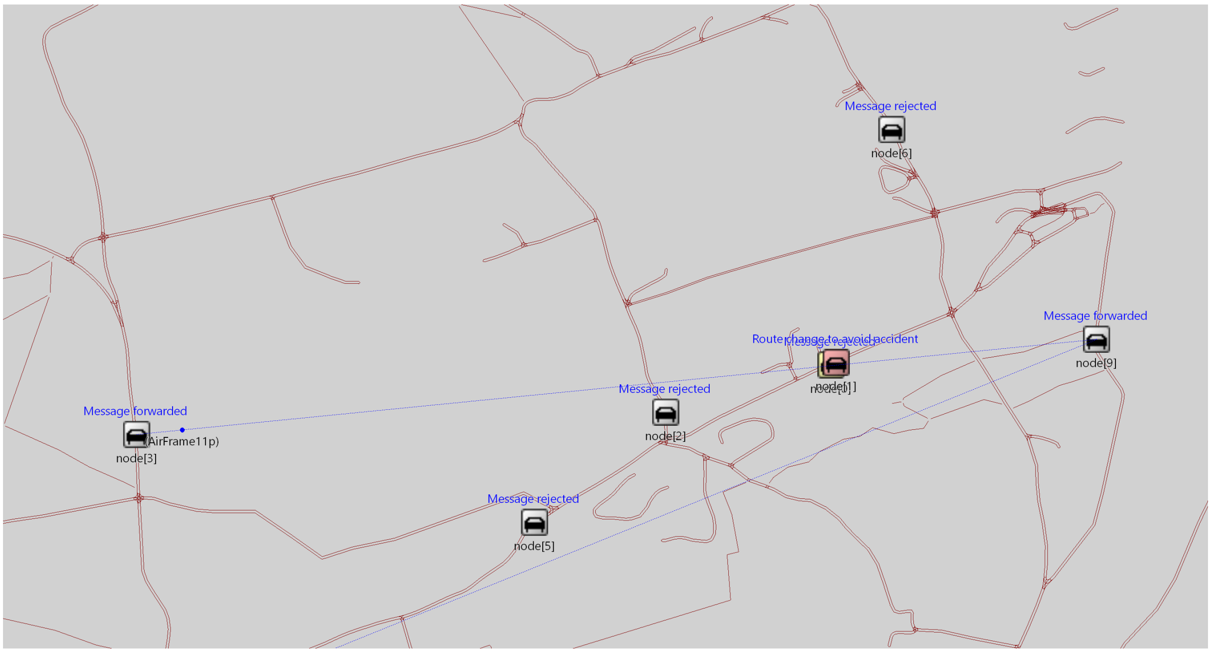


Figure 3. V2V communication scenario exchanging alert messages during accident

score is greater than the threshold. The sender is a trusted vehicle. The receiver accepts the ALERT and generates a route change request.

The Attack Process: If the node is set as a malicious node, beside the above functionalities, it invokes an attack generation method. Depending on the attack parameters (Start time and duration), the attacker broadcasts false alert during the attack period. The broadcast is done every 2 seconds. The parameters (Attack start time, duration, number of node, attack frequency) can be modified according to the testing scenario. In this work, a reputation system help vehicles to make the right decision about how to respond to emergency messages. If a trusted vehicle, see Figure 5 sends an emergency message about an accident, other vehicles can rely on its reputation to assess the urgency and severity of the situation and take appropriate actions. On the other hand, if an untrusted or malicious vehicle, see Figure 4 sends a message that contradicts the information provided by trusted vehicles, other vehicles can disregard the message based on the sender's poor reputation.

5. Results

This section provides a comparative study of two different experiments of vehicle reputation distribution with a variable percentage of malicious vehicles. See Figures 5 and 4 . Key performance metrics, including accepted messages, rejected messages, route changes, and dropped packets-are analyzed to assess system reaction to malicious behavior and message reliability.

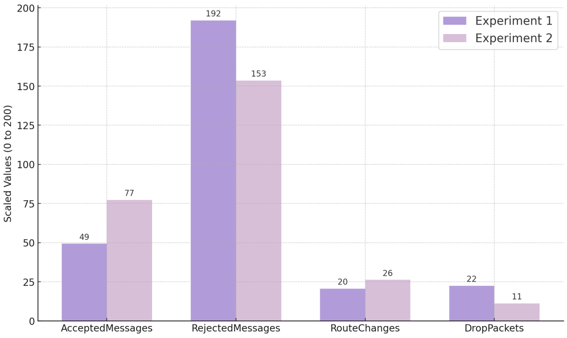


Figure 4. Messages transmission with the impact of 20% malicious vehicles

While Experiment 1 represents a more varied trust environment by using a mix of low and high RVs for all the vehicles, Experiment 2 represents more trusted communications, as generally higher RVs are used for the vehicles. These differences are reflected by the graphs especially in the presence of malicious vehicles. In Experiment 1, the graph shows a remarkably high amount of dropped packets and rejected messages resulting from the mixture of low-RVs that make the system more vulnerable to misbehavior for 20% of malicious vehicles. The second experiment performed better dropped packets were fewer, along with the message rejections, due to the overall higher reputation.

Both experiments are improved by reducing the malicious vehicle percentage to 5%, but Experiment

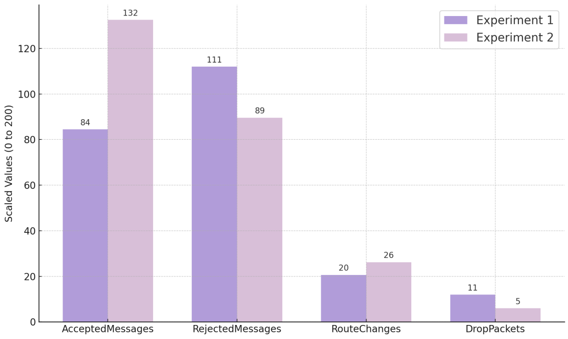


Figure 5. Messages transmission with the impact of 5% malicious vehicles

2 outperforms, showing an increasing number of accepted messages with fewer rejected messages, and fewer dropped packets compared to Experiment 1, wherein the mixed reputation environment results in slightly higher rejection rates. Regarding route changes, in general, Experiment 1, with mixed RVs, results in fewer route changes; this is because communications with low RVs s are less likely to accept accident alerts, leading to slower responses. Conversely, Experiment 2 has higher-reputation vehicles, and therefore its vehicles make more frequent changes to their routes since they trust accident alerts and act upon them by quickly rerouting themselves. This difference becomes even more obvious as the percentage of malicious vehicles drops down to 5%, with Experiment 2 continuing to show better adaptability.

6. Conclusion

Reputation embedded in V2V communication allows vehicles to identify reliable sources, hence enhancing the dependability of the system. The paper proposes the use of reputation values to resolve conflicting message sets in sparse environments. Vehicles with higher RVs tend to show better performance in accepting valid messages, efficient rerouting, and reducing dropped packets while the malicious vehicle percentage goes down. From the results, it can be deduced that the role of trust management is important in V2V networks. A higher reputation vehicle has more resistance than in an environment with mixed reputation. Simulations have proven the effectiveness in improving incident management and accident detection in sparse infrastructure areas by making transportation safer and more efficient.

7. References

[1] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, “A Security Credential Management System for V2V Communications,” *2013 IEEE Vehicular Networking Conference*, IEEE, 2013, pp. 1-8.

[2] D. Almani, T. Muller, S. Furnell, X. Carpent, and T. Yoshizawa, “A Pre-Signature Scheme for Trustworthy Offline V2V Communication,” *Proceedings of the 14th IFIP International Conference on Trust Management (IFIPTM 2023)*, Amsterdam, The Netherlands, 19–20 October 2023.

[3] D. Almani, T. Muller, X. Carpent, T. Yoshizawa, and S. Furnell, “Enabling Vehicle-to-Vehicle Trust in Rural Areas: An Evaluation of a Pre-Signature Scheme for Infrastructure-Limited Environments,” *Future Internet*, Future Internet Journal, 2024.

[4] Q. Li, A. Malip, K.M. Martin, S.L. Ng, and J. Zhang, “A Reputation-Based Announcement Scheme for VANETs,” *IEEE Transactions on Vehicular Technology*, IEEE, 2012, pp. 4095-4108.

[5] H. El Sayed, S. Zeadally, and D. Puthal, “Design and Evaluation of a Novel Hierarchical Trust Assessment Approach for Vehicular Networks,” *Vehicular Communications*, Elsevier, 2020.

[6] J. Naskath, B. Paramasivan, and H. Aldabbas, “A Study on Modeling Vehicles Mobility with MLC for Enhancing Vehicle-to-Vehicle Connectivity in VANET,” *Journal of Ambient Intelligence and Humanized Computing*, Springer, 2021.

[7] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, “Towards Secure and Practical Consensus for Blockchain-Based VANET,” *Information Sciences*, Elsevier, 2021, pp. 170-187.

[8] V. Agate, S. Author2, and T. Author3, “Reliable Reputation-Based Event Detection in V2V Networks,” *International Conference on Advanced Research in Technologies, Information, Innovation and Sustainability*, Springer Nature Switzerland, Cham, 2023, pp. 1-10.

[9] S. Khan, L. Zhu, X. Yu, Z. Zhang, M.A. Rahim, M. Khan, X. Du, and M. Guizani, “Accountable Credential Management System for Vehicular Communication,” *Vehicular Communications*, Elsevier.

[10] M.A. Simplicio, E.L. Cominetti, H.K. Patil, J.E. Ricardini, and M.V.M. Silva, “The Unified Butterfly Effect: Efficient Security Credential Management System for Vehicular Communications,” *2018 IEEE Vehicular Networking Conference (VNC)*, IEEE, 2018, pp. 1-8.

[11] M. Shurrab, S. Singh, H. Otrok, R. Mizouni, V. Khadkikar, and H. Zeineldin, “An Efficient Vehicle-to-Vehicle (V2V) Energy Sharing Framework,” *IEEE Internet of Things Journal*, IEEE, 2021, pp. 5315-5328.

Appendix B

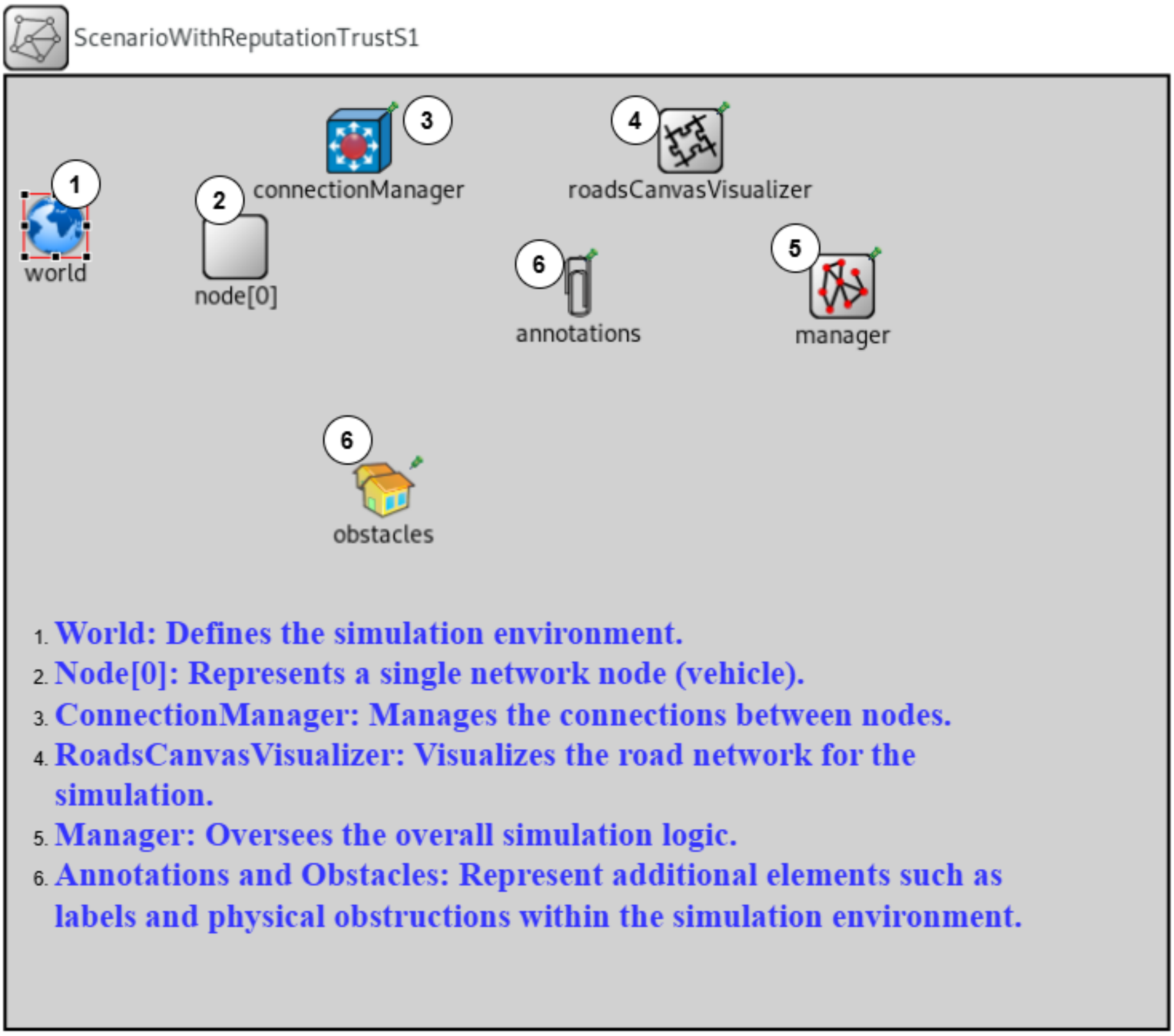
Simulation Overview and Examples

Simulation Environment Snapshots

Overview

This appendix provides a general overview of the simulation environment and the decision-making process in this study. This section briefly shows the main steps involved in the process: network establishment, event detection, Sybil attack initialisation, and decision-making, including reputation and certificate evaluation. The figures overview the essential elements and their interaction with the simulation environment.

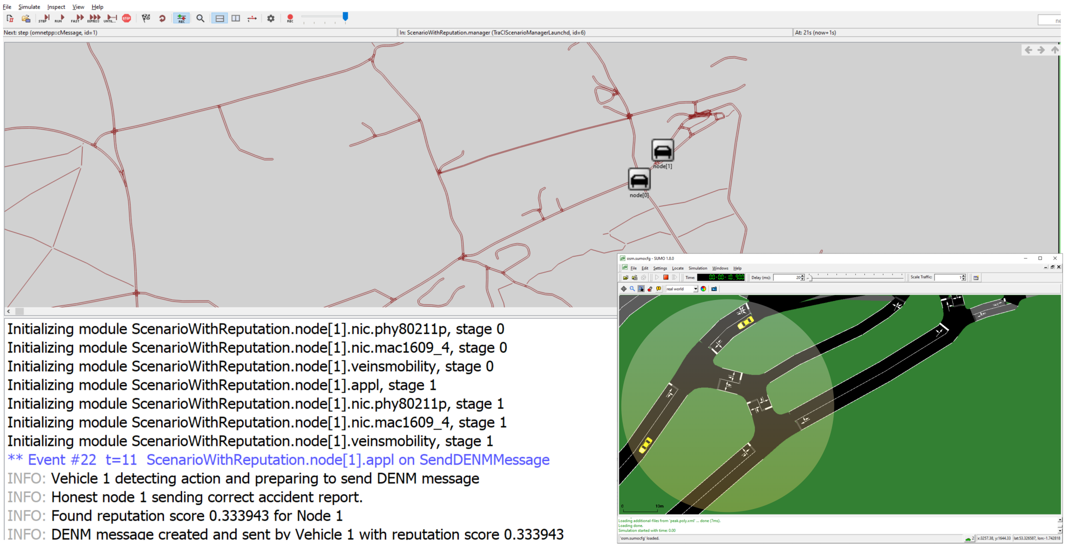
- **Simulation Environment:** Figure 1 depicts the OMNeT++ network topology: a global environment, network node, connection manager handling the communications, and road visualiser representing the network. Obstacles simulate physical barriers, while the manager provides control over the simulation; hence, a dynamic test setup is obtained for the reputation mechanism.



1. World: Defines the simulation environment.
2. Node[0]: Represents a single network node (vehicle).
3. ConnectionManager: Manages the connections between nodes.
4. RoadsCanvasVisualizer: Visualizes the road network for the simulation.
5. Manager: Oversees the overall simulation logic.
6. Annotations and Obstacles: Represent additional elements such as labels and physical obstructions within the simulation environment.

Figure 1: Network Topology in OMNeT++.

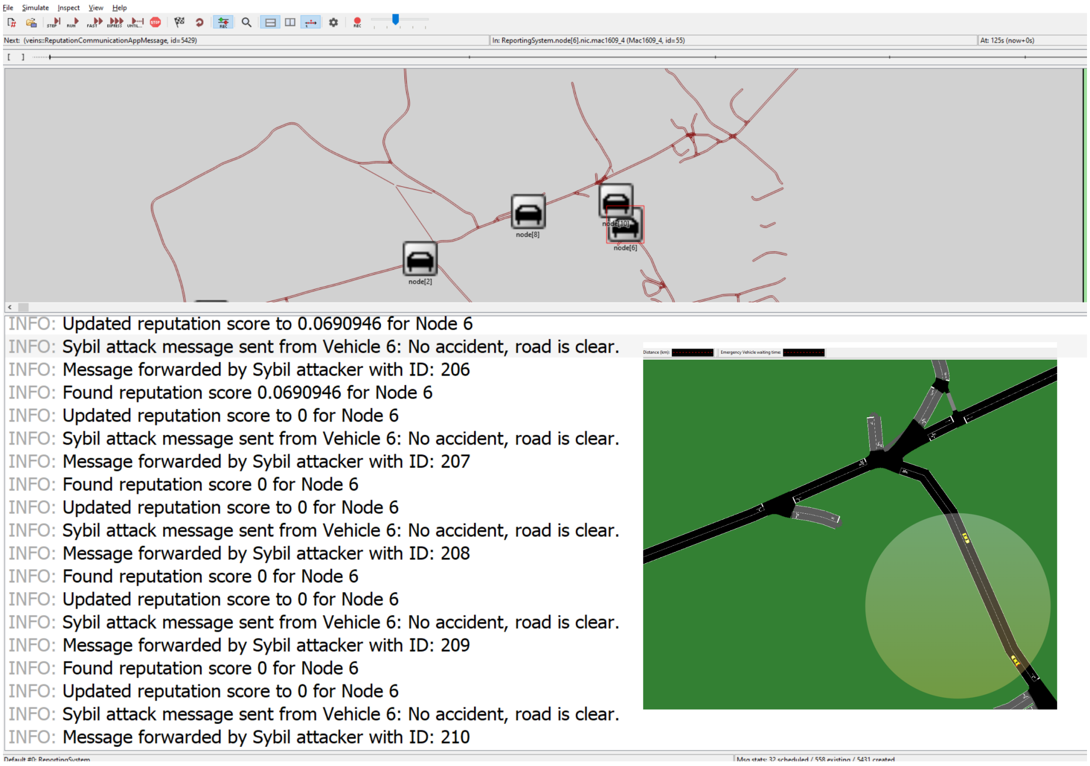
- **Event Detection in Simulation:** Figure 2 represents the event detection. The left side displays the network topology on OMNET++, representing nodes and their connectivity. The console log shows (vehicle 1) detects an accident regarding (Vehicle 0). Vehicle 1 with ($RV = .3$) initialises the DENM message to alert other vehicles. On the right-hand side, a graphical representation on SUMO shows the two vehicles' communication range visualised to demonstrate real-time data exchange and event handling.



```
Initializing module ScenarioWithReputation.node[1].nic.phy80211p, stage 0
Initializing module ScenarioWithReputation.node[1].nic.mac1609_4, stage 0
Initializing module ScenarioWithReputation.node[1].veinsmobility, stage 0
Initializing module ScenarioWithReputation.node[1].appl, stage 1
Initializing module ScenarioWithReputation.node[1].nic.phy80211p, stage 1
Initializing module ScenarioWithReputation.node[1].nic.mac1609_4, stage 1
Initializing module ScenarioWithReputation.node[1].veinsmobility, stage 1
** Event #22  t=11  ScenarioWithReputation.node[1].appl on SendDENMMessage
INFO: Vehicle 1 detecting action and preparing to send DENM message
INFO: Honest node 1 sending correct accident report.
INFO: Found reputation score 0.333943 for Node 1
INFO: DENM message created and sent by Vehicle 1 with reputation score 0.333943
```

Figure 2: Event Detection in Simulation.

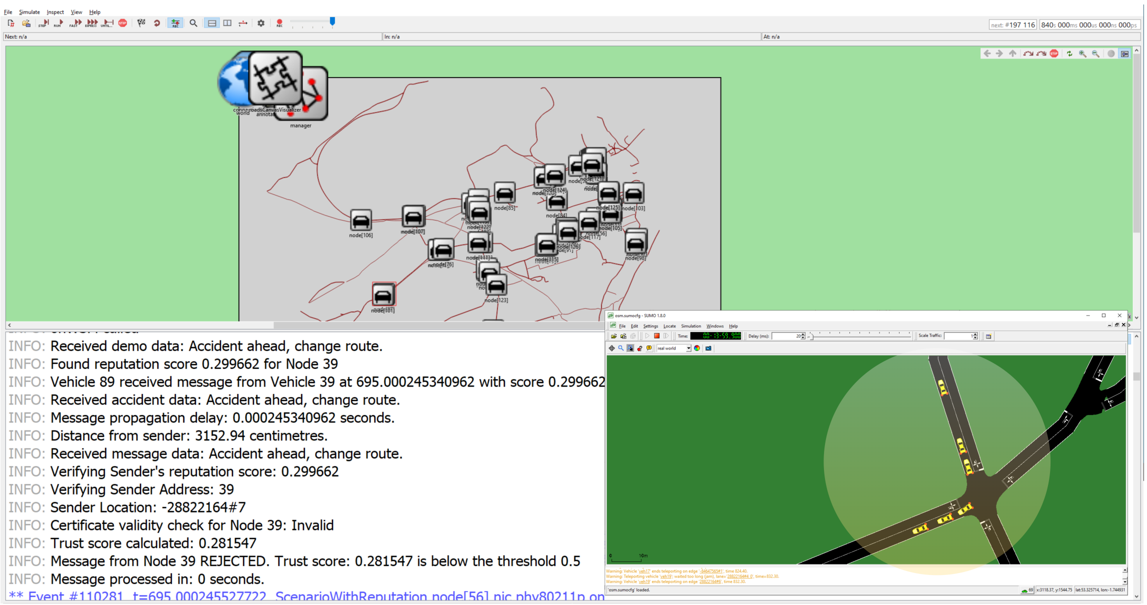
- **Sybil Attack Initiation:** Figure 3 shows the initiation of a Sybil attack (Vehicle 6). Vehicle 6 creates five fake identities (206, 207, 208, 209, 210) to disrupt network communication and propagate false information. The console logs picture the processes occurring during this stage of the simulation.



```
INFO: Updated reputation score to 0.0690946 for Node 6
INFO: Sybil attack message sent from Vehicle 6: No accident, road is clear.
INFO: Message forwarded by Sybil attacker with ID: 206
INFO: Found reputation score 0.0690946 for Node 6
INFO: Updated reputation score to 0 for Node 6
INFO: Sybil attack message sent from Vehicle 6: No accident, road is clear.
INFO: Message forwarded by Sybil attacker with ID: 207
INFO: Found reputation score 0 for Node 6
INFO: Updated reputation score to 0 for Node 6
INFO: Sybil attack message sent from Vehicle 6: No accident, road is clear.
INFO: Message forwarded by Sybil attacker with ID: 208
INFO: Found reputation score 0 for Node 6
INFO: Updated reputation score to 0 for Node 6
INFO: Sybil attack message sent from Vehicle 6: No accident, road is clear.
INFO: Message forwarded by Sybil attacker with ID: 209
INFO: Found reputation score 0 for Node 6
INFO: Updated reputation score to 0 for Node 6
INFO: Sybil attack message sent from Vehicle 6: No accident, road is clear.
INFO: Message forwarded by Sybil attacker with ID: 210
```

Figure 3: Sybil Attack Initiation.

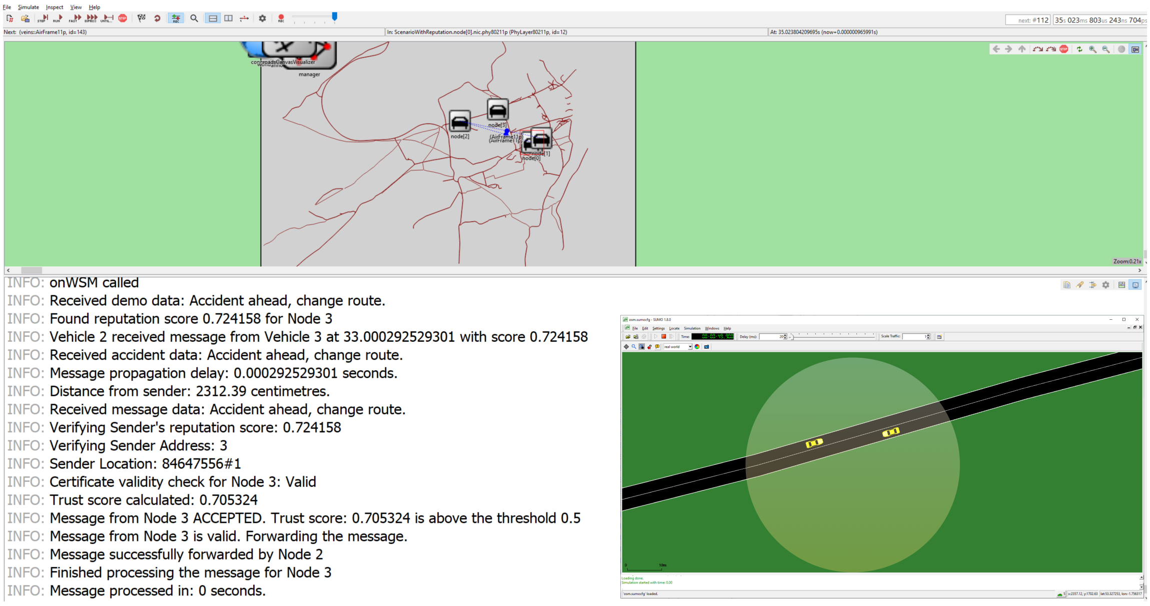
- **Decision-Making in Simulation:** Figures 4 and 5 demonstrate the decision-making outputs in the simulation. The topology on the left side highlights the network structure during these interactions, and the visualization on the right shows the SUMO environment, highlighting the vehicle communications. Two key decisions are assessed below:
  - **Rejection**: Figure 4 shows the rejection of the alert messages received from vehicles with low RV, below the threshold (.5). For example, messages from (vehicle 39) with an RV(0.3) and an invalid certificate are rejected by (Vehicle 89), as seen in the console logs.



```
INFO: Received demo data: Accident ahead, change route.
INFO: Found reputation score 0.299662 for Node 39
INFO: Vehicle 89 received message from Vehicle 39 at 695.000245340962 with score 0.299662
INFO: Received accident data: Accident ahead, change route.
INFO: Message propagation delay: 0.000245340962 seconds.
INFO: Distance from sender: 3152.94 centimetres.
INFO: Received message data: Accident ahead, change route.
INFO: Verifying Sender's reputation score: 0.299662
INFO: Verifying Sender Address: 39
INFO: Sender Location: -28822164#7
INFO: Certificate validity check for Node 39: Invalid
INFO: Trust score calculated: 0.281547
INFO: Message from Node 39 REJECTED. Trust score: 0.281547 is below the threshold 0.5
INFO: Message processed in: 0 seconds.
** Event #110281  t=695.000245527722  ScenarioWithReputation.node[56].nic.phy80211p on
```

Figure 4: Message Rejection Based on Low RV and Invalid Certificate.

- **Accepting**: Figure 5 highlights the alert messages' acceptance and forwarding based on valid certificates and RV exceeding the threshold. For example, messages from (vehicle 3) with an RV(0.7) and a valid certificate are accepted by (Vehicle 2). This acceptance triggers appropriate actions, such as forwarding the message and route changes to avoid an accident, as seen in the console logs.



```
INFO: onWSM called
INFO: Received demo data: Accident ahead, change route.
INFO: Found reputation score 0.724158 for Node 3
INFO: Vehicle 2 received message from Vehicle 3 at 33.000292529301 with score 0.724158
INFO: Received accident data: Accident ahead, change route.
INFO: Message propagation delay: 0.000292529301 seconds.
INFO: Distance from sender: 2312.39 centimetres.
INFO: Received message data: Accident ahead, change route.
INFO: Verifying Sender's reputation score: 0.724158
INFO: Verifying Sender Address: 3
INFO: Sender Location: 84647556#1
INFO: Certificate validity check for Node 3: Valid
INFO: Trust score calculated: 0.705324
INFO: Message from Node 3 ACCEPTED. Trust score: 0.705324 is above the threshold 0.5
INFO: Message from Node 3 is valid. Forwarding the message.
INFO: Message successfully forwarded by Node 2
INFO: Finished processing the message for Node 3
INFO: Message processed in: 0 seconds.
```

Figure 5: Message Acceptance and Forwarding in the Simulation.

Appendix C

Source Code and Simulation Data

All source code and simulation data used in this thesis are available at the following public GitHub repositories:

1. A-Pre-Signature-Scheme-for-Enabling-Vehicle-to-Vehicle-Trust-in-Rural-Areas.
2. Reputation-Based-Decision-Accuracy-in-V2V-Communication-with-Limited-Infrastructure.
3. Distributed-Reputation-for-Accurate-Vehicle-Misbehaviour-Reporting-DRAMBR-.