

Università di Genova

Department of Naval, Electrical, Electronic and Telecommunications Engineering (DITEN)

PhD Program in Science and Technology for Electronic and Telecommunication Engineering (STIET)

Risk-based Cybersecurity Assessment for Vehicle to Everything (V2X) Communications: A Multi-Tier Experimental Framework

PhD Dissertation

by

Muhammad Saad Sohail

Advisor:	Prof. Fabio Patrone
Advisor:	Prof. Mario Marchese
Company Advisor:	Ing. Stefano Delucchi
Co-advisor:	Ing. Giovanni Battista Gaggero
Head of the PhD program:	Prof. Maurizio Valle
Reviewer 1:	Prof. Enrico Cambiaso
Reviewer 2:	Prof. Michele Luglio

Date: 06 - March - 2026

Academic Year 2022-2025, XXXVIII Cycle

Università di Genova | DITEN DIPARTIMENTO DI INGEGNERIA NAVALE, ELETTRICA, ELETTRONICA E DELLE TELECOMUNICAZIONI

Abstract

Connected vehicles promise transformative safety improvements through Vehicle to Everything (V2X) wireless communication, yet the broadcast nature of these networks, heterogeneous protocol integration (DSRC, C-V2X, GNSS, CAN), and millisecond latency safety requirements introduce cybersecurity challenges fundamentally different from enterprise IT contexts. Current vulnerability assessment methods fall short in three ways: simulations miss physical layer attack vectors, hardware testbeds cannot scale economically, and conventional IT security frameworks prioritize confidentiality over the availability and integrity critical for preventing collisions. Bridging these gaps demands adapted methodologies validated across multiple experimental paradigms.

This central contribution of this research addresses the cybersecurity challenges inherent in heterogeneous Vehicle to Everything (V2X) communication environments, where protocol diversity across DSRC, C-V2X, GNSS, and in-vehicle networks creates complex and exploitable vulnerabilities. To enable realistic and scalable experimentation, a comprehensive multi tier testbed architecture was developed, integrating distinct yet complementary validation layers. The first layer employs Software Defined Radio (SDR) platforms to emulate physical layer attacks that cannot be effectively represented in simulation. The second layer incorporates industrial grade Cohda Wireless equipment to ensure applicability and consistency with commercial V2X deployments, The third layer the CyberVehiCare hardware in the loop testbed, facilitates intermediate scale testing under realistic vehicular operating conditions. The integrated framework revealed multiple cross protocol vulnerabilities that are typically undetected by isolated or single paradigm approaches. To systematically assess their impact, a Safety Impact Scoring (SIS) mechanism was introduced, aligned with ISO/SAE 21434 standards, enabling quantifiable evaluation of the physical consequences of communication breaches. Furthermore, a Graph Neural Network (GNN) based intrusion detection system was developed to operate at the physical layer, thereby supporting real time mitigation.

In addition, a hands on cybersecurity training framework strengthening workforce readiness for automotive cybersecurity engineering. Collectively, these contributions span vulnerability discovery, risk quantification, real time detection, and organizational competence development providing holistic V2X cybersecurity solutions bridging academic research and automotive industry deployment needs.

Keywords: V2X Communications, Cybersecurity, Vulnerability Assessment, Software-Defined Radio, Machine Learning, DSRC, C-V2X, Testbed Validation, Physical Layer Security, Risk Management

Contents

Abstract iii

List of Figures x

List of Tables xi

List of Acronyms xiii

List of Notations xix

1 Introduction 1
- 1.1 Background and Motivation . . . 1
- 1.2 Introduction to V2X Communication Framework . . . 2
  - 1.2.1 V2X Security Assessment: State of the Art and Research Gap 2
- 1.3 Research Problem Statement . . . 3
- 1.4 Research Objectives and Methodological Framework . . . 5
- 1.5 Contributions of the Study . . . 7
- 1.6 Thesis Organization . . . 8
- 1.7 Conclusion . . . 10

2 V2X Communication Systems: Protocols and Technologies 13
- 2.1 Introduction . . . 13
- 2.2 V2X Communication Ecosystem Foundation . . . 13
- 2.3 Access Technologies and Physical Layer Analysis . . . 17
  - 2.3.1 IEEE-802.11p/DSRC Systems Architecture . . . 17
  - 2.3.2 Cellular V2X Technologies (LTE-V2X and 5G NR-V2X) . . . 19
  - 2.3.3 Physical Layer Parameters and Performance Analysis . . . 21
  - 2.3.4 Comparative Technology Assessment . . . 22
- 2.4 Protocol Stack Architecture and Implementation . . . 22
  - 2.4.1 WAVE Protocol Stack (IEEE 1609.x Series) . . . 22
  - 2.4.2 ETSI ITS G5 Protocol Implementation . . . 23
  - 2.4.3 3GPP C-V2X Protocol Architecture . . . 24
  - 2.4.4 Cross Stack Interoperability Analysis . . . 25
- 2.5 Multi Channel Coordination and Resource Management . . . 25
  - 2.5.1 IEEE 1609.4 Multi Channel Operation . . . 25
  - 2.5.2 DCC mechanisms . . . 27
  - 2.5.3 Resource Allocation in C-V2X . . . 29
  - 2.5.4 Performance Optimization Strategies . . . 30
- 2.6 Security and Privacy Framework . . . 30

2.6.1 IEEE 1609.2 Security Services 30
2.6.2 ETSI Security Architecture and PKI 31
2.6.3 Certificate Management and Pseudonym Systems 32
2.6.4 Cross Technology Security Interoperability 32
2.6.5 Integrity and Non-Repudiation in V2X PKI 33
2.6.6 Deployment Status and Interoperability 33
2.6.7 V2X Service Classification and Requirements 34
2.7 Regulatory Framework and Spectrum Management 35
2.7.1 Regional Spectrum Allocations 36
2.7.2 Regulatory Compliance Requirements 36
2.7.3 Cross Border Interoperability Challenges 37
2.8 Implementation Challenges and Research Directions 37
2.8.1 Scalability and Performance Limitations 38
2.8.2 Security Implementation at Scale 38
2.8.3 Cross Technology Coexistence 39
2.8.4 Future Research Opportunities 39
2.9 Chapter Summary and Integration 40

3 V2X cybersecurity Risk Management 43
3.1 Introduction 43
3.2 Fundamental Concepts of V2X cybersecurity Risk Management . . . 44
3.2.1 Regional Security Framework Differences 48
3.2.2 V2X-Specific Security Characteristics 48
3.2.3 Cause-Effect-Consequence Framework 51
3.3 Context and Scope Definition for V2X Risk Management 52
3.3.1 Compliance with Security Standards 52
3.3.2 Operational Boundary Definition 55
3.4 Risk Assessment for V2X Systems 57
3.4.1 Risk Identification 57
3.4.2 Risk Analysis and Quantitative Assessment 58
3.4.3 V2X-Specific Risk Parameterization 61
3.5 Risk Treatment and Mitigation for V2X Systems 63
3.5.1 Cryptographic Protection and Authentication 63
3.5.2 Intrusion Detection and Anomaly Detection 66
3.5.3 Redundancy and Multi-Channel communication 69
3.5.4 Secure Protocol Design and Standardization 69
3.5.5 Misbehavior Detection and Response Systems 69
3.5.6 Organizational and Procedural Measures 69
3.6 Continuous Monitoring and Review for V2X Risk Management 70
3.6.1 Key Monitoring Mechanisms 72
3.6.2 Review and Adaptation 72
3.6.3 Adaptive Security Measures 73
3.6.4 Regulatory Compliance and Audit Requirements 73
3.7 Conclusion 73

4 Multi Tier Testbed Framework for V2X Security Assessment 75
4.1 Regional Security Framework 76
4.2 Related Works: Vulnerability Assessment in V2X Communication . . 77
4.3 Security Challenges in V2X 80
4.4 Reference Architecture and Testbed Design 80
4.4.1 Tier 1: SDR-Based Emulation Testbed 81
4.4.2 Tier 2: Industrial V2X Equipment Testbed 85
4.4.3 Hardware Architecture and Capabilities 85
4.4.4 Synchronization, Timing, and Location 86
4.4.5 Software Framework and Development Environment 87
4.5 Potential V2X Attack Scenarios within the Systematic Vulnerability Assessment Framework 88
4.6 Framework implementation architecture 92
4.6.1 SDR-Based Security Assessment Tool 92
4.6.2 Reproducibility and Open Source Implementation 94
4.6.3 Selected Attack Scenarios for Framework Validation 95
4.6.4 Denial of Service through Jamming 95
4.6.5 Replay attack 96
4.6.6 Complex Attacks 98
4.7 Experimental Evaluation of the Framework Using Selected Attacks . 99
4.7.1 Jamming Attack 99
4.7.2 Replay Attack 101
4.8 Conclusion 103

5 Vulnerability monitoring trough SDR-DL in Physical Layer Security for C-V2X Communications 105
5.1 Introduction to Vulnerability Monitoring in C-V2X PLS 106
5.2 Physical Layer Threat Model and Attack Vectors 107
5.2.1 C-V2X Spoofing Attack Taxonomy 108
5.2.2 Signal Characteristics Exploitation 108
5.2.3 Advanced Persistent Threats Targeting Physical Layer Features 110
5.2.4 Cross Layer Attack Correlation and Propagation 110
5.3 Proposed SDR Architecture for C-V2X Monitoring 111
5.3.1 SDR Interface, Architecture, and Signal Acquisition for C-V2X Monitoring 114
5.3.2 SDR Interface and Libraries 114
5.3.3 SDR Architecture for C-V2X Monitoring 114
5.3.4 Real time Signal Acquisition and Processing 115
5.3.5 Feature Extraction Methodologies 116
5.3.6 Hardware Considerations for Deployment Architectures 117
5.4 Proposed framework of ML Approaches for Anomaly Detection 117
5.4.1 Deep Neural Network Position Change Detector Implementation 118
5.4.2 Graph Neural Network Analysis for Temporal Pattern Recognition 120
5.4.3 Multi Feature Fusion Techniques for Enhanced Detection Accuracy 121
5.5 Implementation Challenges and Performance Optimization 122
5.5.1 Computational Complexity Management in real time Systems 122

5.5.2 Environmental Noise and Channel Variation Mitigation 124
5.5.3 Scalability Considerations for Dense Vehicular Networks . . . 124
5.5.4 Edge Computing Integration for Distributed Monitoring . . . 125
5.6 Proposed framework implementation for Graph Construction using PCD Outputs 126
5.7 GNN Implementation for Spoofing Classification 127
5.8 System Integration and Performance Evaluation in Simulation 129
5.9 Conclusion 130

6 Cybersecurity Awareness Research and Training in V2X Sector 135
6.1 Introduction to Cybersecurity Awareness in Automotive V2X Systems 135
6.1.1 The Paradigm Shift: From Mechanical Safety to Cyber-Physical Security 135
6.1.2 The Human Factor: Why Technical Solutions Are Not Sufficient 138
6.1.3 Chapter Scope and Research Questions 139
6.2 Research Landscape: Cybersecurity Training Methodologies for V2X . 140
6.2.1 Cyber Ranges and Testbeds: Taxonomy and Evolution 140
6.2.2 Automotive Cybersecurity Testbeds: State of the Art 142
6.2.3 V2X Specific Training Requirements and Challenges 144
6.3 CyberVehiCare: A Case Study in Research-Driven Cybersecurity Training 147
6.3.1 Testbed Architecture and Dual Purpose Design 148
6.4 Validation Framework 152
6.4.1 Data Capture and Display 152
6.4.2 Command Execution from External Interface 153
6.4.3 Deactivation and Security Commands 154
6.4.4 Validation Summary 154
6.5 Training Capabilities and Modules 156
6.5.1 In-Vehicle Network Security 156
6.5.2 V2X Communication Security 158
6.6 Awareness Framework Implementation and Validation 160
6.6.1 Three Tier Competence Framework Architecture 160
6.6.2 Continuous Monitoring and Feedback 162
6.7 Challenges and Future Directions in V2X Cybersecurity Training . . 163
6.7.1 Current Limitations and Barriers 163
6.7.2 Emerging Solutions and Innovations 164
6.7.3 Future Research Directions 166
6.8 Conclusions 167

7 Conclusions and Future Directions 171
7.1 Introduction 171
7.2 Synthesis of Contributions 172
7.3 Research Questions Revisited 175
7.4 Theoretical Contributions to Academic Knowledge 178
7.5 Practical Implications for Industry and Policy 179

Acknowledgments 207

List of Figures

2.1 Autonomous Connected vehicle equipped with sensors for decision making while driving . . . 14
2.2 V2X Communication Ecosystem Architecture . . . 15
2.3 Architecture of Vehicle to Everything (V2X) [1] . . . 17
2.4 A comparative analysis of V2X access technologies . . . 18
2.5 DSRC-based V2X communications architecture . . . 19
2.6 General architecture of C-V2X network . . . 20
2.7 Transmission modes of V2X . . . 20
2.8 Protocol Stack Architecture Comparison . . . 23
2.9 Multi Channel Coordination Timing framework . . . 26
2.10 DCC state machine showing transitions between Relaxed, Active and Restrictive states . . . 28
2.11 Global V2X Spectrum Allocations and Regulatory Framework. . . . 35

3.1 V2X Risk Management Framework . . . 45
3.2 V2X Asset Classification and Threat Landscape Analysis . . . 47
3.3 Comprehensive Security Standards Compliance Matrix mapping regulatory requirements to implementation strategies . . . 54
3.4 Quantitative Risk Assessment Model for V2X Systems. . . . 59
3.5 Multi-layered V2X Security Architecture . . . 65
3.6 V2X IDS Architecture . . . 67
3.7 Comparative performance Analysis of V2X security mechanism . . . 68
3.8 Continuous Risk Monitoring and Adaptive Cycle for V2X . . . 71

4.1 GNU Radio flowgraph implementation of OBU . . . 82
4.2 GNU Radio flow graph implementation of the RSU . . . 84
4.3 MK6 Cohda Wireless OBU and RSU Testbed for Industrial V2X Communication Systems. . . . 86
4.4 Flow chart(decision tree) of the vulnerability assessment framework proposed. . . . 89
4.5 SDR-based security assessment tool: System architecture showing dual SDR configuration for simultaneous attack generation and monitoring. 93
4.6 System architectures of the implemented emulation testbed (**left**) and industrial testbed (**right**) for V2X communications. . . . 94
4.7 SDR-based security assessment tool: Monitor interface showing received packet list (**left**) and signal analysis with time domain representation and BPSK constellation plot (**right**) during normal IEEE 802.11p packet transmissions. . . . 94
4.8 SDR-based security assessment tool: Attacker flow graph . . . 97

4.9 SDR-based security assessment tool: Replay attack implementation using for IQ sample capture with file storage 98
4.10 SDR-based security assessment tool: Monitor interface during jamming attack showing disrupted packet reception (**left**) and severely distorted constellation plot with scattered points indicating signal corruption (**right**). 99
4.11 SDR-based security assessment tool: Monitor interface during replay attack, captured packet analysis through Wireshark (**left**) and normal constellation plot (**right**) indicating successful message injection. . . . 101
4.12 System logs from RSU in Industrial testbed showing successful processing of legitimate IVI message (green highlight) and rejection of replayed IVI message due to failed sanity checks (red highlight). . . . 102
4.13 System logs from OBU in Industrial testbed with DENM processing (green highlight) and timestamp validation failure for replayed DENM message (red highlight). 102

5.1 Framework Overview 107
5.2 Attack taxonomy visualization. 109
5.3 SDR-based Monitoring Architecture for C-V2X systems. 112
5.4 PCD neural network architecture. 119
5.5 Performance optimization framework. 123
5.6 PCD Training History (Accuracy and Loss) 131
5.7 GNN Confusion Matrix on Test Set 131

6.1 Automotive cybersecurity evolution timeline. 136
6.2 V2X attack surface taxonomy. 137
6.3 V2X attack layer taxonomy mapping threats. 146
6.4 CyberVehiCare prototype testbed Architecture. 147
6.5 Block diagram of the testbed. 148
6.6 CyberVehiCare testbed training architecture. 150
6.7 Foglight dashboard after trigger. 152
6.8 Instrument after trigger. 152
6.9 Graph diagram of ambient temperature 153
6.10 Graph diagram of accelerator pedal 153
6.11 Fog light status 155
6.12 Ambient Temperature Sensor Status 155

List of Tables

2.1 Comparative Physical Layer Parameters for V2X Access Technologies 21
2.2 V2X Service Category Summary with Performance Requirements . . 34

3.1 Cross-Domain Latency Comparison for Safety-Critical Wireless Systems 52
3.2 Enhanced V2X Attack Taxonomy with Protocol-Specific Threat Manifestations 60

4.1 V2X System Layers, IP Stack Mapping, Potential Threats, and Mitigation Approaches 78
4.2 Experimental parameters for security assessment tests. 88

5.1 Comparison of SDR Interface Libraries 115

6.1 Cyber Range Taxonomy for V2X Training 141
6.2 Automotive Testbed Feature Comparison 144
6.3 Three Tier V2X Cybersecurity Competence Framework. 162

List of Acronyms

3GPP	3rd Generation Partnership Project
5G	Fifth Generation
AI	Artificial Intelligence
ANN	Artificial Neural Network
API	Application Programming Interface
BSM	Basic Safety Message
BTP	Basic Transport Protocol
CA	Certificate Authority
CAM	Cooperative Awareness Message
CAN	Controller Area Network
CBR	Channel Busy Ratio
CCH	Control Channel
CIA	Confidentiality, Integrity, Availability
C-ITS	Cooperative Intelligent Transportation Systems
CNN	Convolutional Neural Network
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSMA	Carrier Sense Multiple Access
CSMS	Cybersecurity Management System
CSI	Channel State Information
CVSS	Common Vulnerability Scoring System
C-V2X	Cellular Vehicle-to-Everything
DCC	Decentralized Congestion Control
DENM	Decentralized Environmental Notification Message

DNN	Deep Neural Network
DoS	Denial of Service
DSRC	Dedicated Short-Range Communications
ECDSA	Elliptic Curve Digital Signature Algorithm
ECU	Electronic Control Unit
EDCA	Enhanced Distributed Channel Access
ETSI	European Telecommunications Standards Institute
FFT	Fast Fourier Transform
FPGA	Field Programmable Gate Array
GNN	Graph Neural Network
GNSS	Global Navigation Satellite System
GNU	GNU's Not Unix
GPS	Global Positioning System
GRU	Gated Recurrent Unit
HSM	Hardware Security Module
IEEE	Institute of Electrical and Electronics Engineers
IMU	Inertial Measurement Unit
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
ITS	Intelligent Transportation Systems
ITS-G5	ITS operating in 5 GHz band
KPI	Key Performance Indicator
LAN	Local Area Network
LiDAR	Light Detection and Ranging
LIN	Local Interconnect Network
LSTM	Long Short-Term Memory
LTE	Long-Term Evolution
MAC	Medium Access Control

MEC	Multi-Access Edge Computing
MIPS	Million Instructions Per Second
ML	Machine Learning
NAS	Non-Access Stratum
NFV	Network Functions Virtualization
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NR	New Radio
NR-V2X	New Radio Vehicle-to-Everything
ns-3	Network Simulator 3
OBD	On-Board Diagnostics
OBU	On-Board Unit
OCB	Outside the Context of a BSS
OFDM	Orthogonal Frequency-Division Multiplexing
OEM	Original Equipment Manufacturer
OMNeT++	Objective Modular Network Testbed in C++
OTA	Over-The-Air
PC5	Sidelink Interface in LTE/5G
PCD	Position-Change Detector
PDR	Packet Delivery Ratio
PHY	Physical Layer
PKI	Public Key Infrastructure
PLS	Physical Layer Security
P-ITS-S	Personal ITS Station
PSSCH	Physical Sidelink Shared Channel
QPSK	Quadrature Phase-Shift Keying
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RADAR	Radio Detection and Ranging

RAN	Radio Access Network
RF	Radio Frequency
ReLU	Rectified Linear Unit
R-ITS-S	Roadside ITS Station
RNN	Recurrent Neural Network
ROI	Return on Investment
RSU	Roadside Unit
RSSI	Received Signal Strength Indicator
SAE	Society of Automotive Engineers
SAM	Smart Agricultural Machine
SBAS	Satellite-Based Augmentation System
SCH	Service Channel
SCMS	Security Credential Management System
SDN	Software-Defined Networking
SDR	Software-Defined Radio
SHA	Secure Hash Algorithm
SINR	Signal-to-Interference-plus-Noise Ratio
SNR	Signal-to-Noise Ratio
SUMO	Simulation of Urban Mobility
TARA	Threat Analysis and Risk Assessment
TCU	Telematics Control Unit
TDMA	Time Division Multiple Access
TLS	Transport Layer Security
TMC	Traffic Management Center
TN	True Negative
TP	True Positive
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UE	User Equipment

UNECE	United Nations Economic Commission for Europe
USRP	Universal Software Radio Peripheral
UTC	Coordinated Universal Time
V2C	Vehicle-to-Cloud
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VANET	Vehicular Ad Hoc Network
V-ITS-S	Vehicle ITS Station
VRU	Vulnerable Road User
WAVE	Wireless Access in Vehicular Environments
WLAN	Wireless Local Area Network
WSMP	WAVE Short Message Protocol

List of Notations

f_c Carrier frequency (Hz)

B Bandwidth (Hz)

P_{tx} Transmission power (dBm)

P_{rx} Received power (dBm)

G_{tx} Transmit antenna gain (dBi)

G_{rx} Receive antenna gain (dBi)

d Distance between transmitter and receiver (m)

λ Wavelength (m)

$RSSI$ Received Signal Strength Indicator (dBm)

SNR Signal-to-Noise Ratio (dB)

$SINR$ Signal-to-Interference-plus-Noise Ratio (dB)

N_0 Noise power spectral density (dBm/Hz)

τ Propagation delay (s)

T Message generation interval (s)

L Packet/message length (bytes)

R Data rate (Mbps)

α Path loss exponent

σ Shadow fading standard deviation (dB)

PDR Packet Delivery Ratio (%)

Δt Latency/end-to-end delay (ms)

T_{proc} Processing time (ms)

T_{prop} Propagation time (ms)

T_{queue} Queuing delay (ms)

N Number of vehicles/nodes

ρ Vehicle density (vehicles/km)

v Vehicle velocity (km/h)

a Acceleration (m/s^2)

θ Heading angle (degrees)

x, y Position coordinates (m)

CBR Channel Busy Ratio (%)

η Detection accuracy (%)

FPR False Positive Rate (%)

FNR False Negative Rate (%)

$\mathcal{L}$ Loss function

W Weight matrix

b Bias vector

$\sigma(\cdot)$ Activation function

$\mathcal{G}(V, E)$ Graph with vertices V and edges E

A Adjacency matrix

H Hidden state/feature matrix

β Learning rate

ϵ Threshold parameter

Chapter 1

Introduction

1.1 Background and Motivation

Road traffic accidents constitute a persistent global public health crisis.The World Health Organization reports that road traffic injuries cause approximately 1.35 million deaths globally each year, with 93% of these fatalities occurring in low and middle-income countries despite these nations accounting for only 60% of the world's vehicles. In the United States, the National Highway Traffic Safety Administration documented over 42,000 traffic fatalities in 2021, representing a 10.5% increase from the previous year and the highest annual toll since 2005 [2, 3]. Beyond the human toll, traffic incidents impose substantial economic burdens through medical expenditures, property damage, and productivity losses. These stark realities have catalyzed extensive academic and industrial research into advanced safety mechanisms designed to mitigate vehicular collision risks. Among the most promising technological responses is the Intelligent Transportation System (ITS) paradigm, which leverages ubiquitous wireless connectivity to enable real time information exchange among vehicles, infrastructure elements, and pedestrians [4].

ITS architectures facilitate the dissemination of safety critical data including geographic positioning, velocity vectors, directional intent, and hazard warnings, thereby augmenting situational awareness for human drivers and autonomous control systems alike [5]. Through cooperative perception and distributed decision making, ITS platforms hold potential to substantially reduce accident rates, optimize traffic flow, and enable advanced mobility services. The integration of autonomous driving technologies within ITS frameworks has further amplified research interest in assessing their combined efficacy for safety enhancement and transportation system efficiency.

However, the proliferation of wireless and cellular communication technologies within vehicular networks introduces cybersecurity vulnerabilities absent from conventional transportation infrastructure. The inherent openness of wireless channels, coupled with the broadcast nature of safety messages, exposes Vehicle to Everything (V2X) systems to threats including eavesdropping, message manipulation, identity spoofing, and Denial of Service (DoS) attacks [3]. Unlike static wireless networks, vehicular environments exhibit high node mobility, frequent topology changes, and stringent real time constraints, necessitating sophisticated communication protocols and computational capabilities. These characteristics render V2X systems particularly attractive targets for adversarial actors seeking to compromise traffic safety, privacy, or system availability. Addressing these cybersecurity challenges requires

systematic vulnerability assessment methodologies tailored to the unique operational and safety critical nature of vehicular communications.

1.2 Introduction to V2X Communication Framework

V2X communication encompasses the suite of wireless technologies enabling information exchange within ITS, including Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Pedestrian (V2P), and Vehicle to Network (V2N) modes [6]. Unlike conventional wireless networks, V2X systems must satisfy stringent performance requirements: ultra low latency (<100 ms for safety messages), high reliability (>95% packet delivery ratio), and seamless operation amid extreme mobility patterns (relative velocities exceeding 500 km/h in opposing traffic scenarios) [7]. These requirements are addressed through a heterogeneous protocol ecosystem spanning multiple communication layers and technologies.

Contemporary V2X deployments integrate diverse protocol families, each serving distinct functional roles. Dedicated Short Range Communication (DSRC) based on IEEE 802.11p provides low latency broadcast messaging for safety applications [8], complemented by Cellular V2X (CV2X) technologies that leverage LTE and 5G New Radio infrastructure for extended range and high throughput connectivity [9]. Within vehicles, the Controller Area Network (CAN) bus facilitates real time communication among electronic control units, sensors, and actuators. Global Navigation Satellite Systems (GNSS) furnish positioning and timing synchronization, while short range technologies such as Bluetooth enable in-vehicle connectivity. Higher layer protocols including IEEE 1609.x (WAVE networking and security services) [10–12], SAE J2735 (message set dictionary) [11], and ETSI standards (Cooperative Awareness Messages - CAM, Decentralized Environmental Notification Messages - DENM) [13, 14] define message formats and security mechanisms. This multi layered, heterogeneous architecture detailed in depth in Chapter 2 creates complex interdependencies that substantially expand the attack surface available to potential adversaries.

1.2.1 V2X Security Assessment: State of the Art and Research Gap

The critical importance of V2X cybersecurity has motivated substantial research into vulnerability assessment methodologies and testbed development. Existing approaches can be categorized into three primary paradigms, each exhibiting distinct strengths and limitations that inform the research gap addressed by this thesis.

Simulation based approaches employ network simulation frameworks such as Veins [15], ns3, and OMNeT++ coupled with traffic simulators including SUMO to achieve large scale scenario modeling (10,000+ vehicles). These platforms excel in scalability and reproducibility, enabling rapid exploration of protocol behavior under diverse traffic densities and attack scenarios. However, simulation based methodologies systematically abstract physical layer characteristics, omitting radio frequency propagation effects, channel impairments, and signal level vulnerabilities. Consequently, attacks exploiting physical layer properties including reactive jamming, signal manipulation, and channel state exploitation remain inadequately captured.

Furthermore, simulation environments typically model idealized protocol implementations, diverging from the behavioral nuances of commercial V2X hardware and software stacks.

Hardware based testbeds utilizing commercial V2X equipment (Cohda Wireless MK6, Savari StreetWAVE, Commsignia Road Side Units) provide high fidelity validation with industrial grade implementations. These platforms capture real world protocol behaviors, hardware specific vulnerabilities, and genuine RF propagation characteristics. However, hardware testbeds suffer from severe scalability constraints due to equipment costs ($15,000–$30,000 per On Board Unit) and logistical complexity, typically supporting fewer than 10 simultaneous nodes. Additionally, commercial platforms often restrict access to internal protocol stack implementations, limiting the feasibility of fine grained vulnerability analysis and attack emulation.

Software Defined Radio (SDR) approaches offer intermediate solutions by enabling flexible, programmable radio implementations using platforms such as USRP, LimeSDR, and HackRF [16]. SDR based testbeds facilitate physical layer experimentation, signal level attack emulation, and protocol stack customization at substantially lower cost than commercial hardware. Recent efforts have demonstrated IEEE 802.11p transceiver and receiver implementations using GNU Radio and evaluated specific attack vectors including beacon spoofing and replay attacks. However, existing SDR based V2X research has not systematically integrated large scale traffic simulation, multi tier validation with commercial hardware, or comprehensive safety impact assessment frameworks.

This literature reveals a critical gap that no existing methodology integrates SDR based physical layer emulation, large scale traffic simulation, and industrial hardware validation within a unified framework addressing both technical vulnerabilities and safety critical impacts. Existing approaches trade off scalability against fidelity, or physical layer realism against system level safety assessment. Traditional vulnerability assessment methodologies developed for enterprise IT systems prioritize confidentiality within the CIA triad, whereas V2X systems invert this hierarchy, emphasizing availability and integrity due to their safety critical nature [17]. This fundamental difference necessitates adapted assessment frameworks incorporating V2X specific metrics including latency degradation, cooperative awareness disruption, and safety message integrity. The present research addresses these gaps through three tier testbed integration and novel vulnerability assessment adaptations, as detailed in subsequent sections.

1.3 Research Problem Statement

The rapid evolution of V2X communication technologies has enabled promising advances in cooperative driving, collision avoidance, and traffic management; however, the inherent complexity and heterogeneity of these networks present significant security and reliability concerns that remain inadequately addressed by existing methodologies. V2X environments integrate multiple underlying protocols including DSRC (IEEE 802.11p), LTE V2X, 5G NR V2X, GNSS positioning, Bluetooth connectivity, and in-vehicle CAN systems each with distinct operational characteristics, performance requirements, and potential vulnerabilities [6]. The coexistence and interaction of these diverse protocols create a multifaceted attack surface that adversaries may exploit through cross protocol attacks, timing vulnerabilities, or resource

exhaustion techniques.

While cyberattacks targeting wireless and vehicular systems have been demonstrated in isolated research contexts [3, 7], systematic testing capabilities that emulate realistic attack conditions while evaluating their cascading impacts on message integrity, availability, and latency in end-to-end V2X deployments remain absent. Existing vulnerability assessment methodologies typically comprising reconnaissance, threat modeling, exploitation, and reporting phases have proven effective in enterprise network contexts but exhibit critical limitations when applied to vehicular communications [17]. Specifically, traditional approaches inadequately account for high node mobility (relative velocities exceeding 500 km/h), ultra low latency requirements (safety messages requiring $<$100 ms end-to-end delivery), and the direct coupling between communication failures and physical safety outcomes. Furthermore, conventional security assessments prioritize confidentiality within the CIA triad, whereas V2X systems invert this priority structure, emphasizing availability and integrity due to their life critical nature.

There exists, therefore, a pressing need to adapt and extend vulnerability assessment methodologies to accommodate mobility induced topology dynamics, temporal constraints, and the unique adversarial models associated with V2X systems (as analyzed in Chapter 3). This thesis addresses the research problem of developing systematic, experimentally validated frameworks for identifying, assessing, and mitigating vulnerabilities in V2X communication systems through adapted methodologies and multi tier testbed validation spanning simulation, SDR emulation, and industrial hardware platforms (detailed explainations are provided in Chapters 4 and 5). This thesis is guided by three central research questions designed to address both theoretical gaps and practical challenges in the cybersecurity assessment of V2X systems.

1. **What are the fundamental communication protocols that underpin V2X systems, and what security challenges emerge from their heterogeneity and integration?** V2X communications rely on a diverse set of standards and technologies, including IEEE 802.11p for DSRC, LTE V2X and 5G NR V2X for cellular connectivity, and complementary systems such as GNSS and CAN bus [8, 9]. Each protocol exhibits distinct characteristics regarding latency, scalability, reliability, and security mechanisms. The coexistence and interoperability of these heterogeneous technologies create both operational opportunities and security vulnerabilities, raising questions about how their integration exposes novel attack surfaces and cross protocol exploitation vectors. Chapter 2 provides comprehensive technical analysis of these protocol families, identifying specific vulnerabilities that inform the assessment frameworks developed in subsequent chapters.

2. **What testing capabilities and experimental tools are required to realistically simulate, generate, and analyze cyberattacks against V2X environments?** Effective vulnerability assessment depends on experimental capabilities that capture the complexity of vehicular communication environments, including large scale mobility patterns, realistic wireless channel conditions, and diverse attack vectors. This necessitates tools capable of modeling protocol level interactions, emulating physical layer phenomena, and evaluating safety critical impacts under controlled conditions [15]. Chapter 4

addresses this question through development of testbed architecture integrating SDR platforms, hardware in the loop systems, and industrial V2X equipment, while Chapter 5) extends assessment capabilities with machine learning based physical layer monitoring.

3. **How must traditional vulnerability assessment methodologies be modified or extended to improve their applicability, Awareness and Training in the context of V2X systems?** Conventional approaches to vulnerability assessment typically separate protocol level weaknesses from system level impacts, an artificial division insufficient for V2X environments where communication security directly affects road safety and cooperative awareness [17]. Traditional methodologies prioritize confidentiality, whereas V2X systems emphasize availability and integrity due to their safety critical nature. Understanding how to adapt assessment frameworks to incorporate V2X specific metrics including safety impact scoring, real time performance degradation, and cooperative function disruption is essential for advancing vehicular cybersecurity research. Chapter 3 develops these adapted risk management frameworks, validated through the experimental methodologies of Chapters 4 and 5 and by leveraging the CyberVehiCare hardware in the loop testbed described in Chapter 6. This work promotes comprehensive research, capacity building, and awareness in the evolving field of V2X communications and cybersecurity.

1.4 Research Objectives and Methodological Framework

The primary objective of this study is to advance the security and operational resilience of V2X communication systems through systematic vulnerability analysis and the development of comprehensive assessment methodologies tailored to the unique characteristics of vehicular networks. To address this goal, the research pursues four interconnected objectives that collectively fill the current research gap in V2X cybersecurity.

First, the study provides a detailed protocol level security analysis of the core communication technologies underpinning V2X connectivity, encompassing four major protocol families: DSRC, Cellular V2X (LTE-V2X and 5G NR-V2X), GNSS, and in-vehicle CAN bus architectures. Chapter 2, this analysis identifies inherent protocol weaknesses, evaluates cryptographic protection mechanisms, and characterizes vulnerabilities arising from heterogeneous protocol integration within unified vehicular platforms. It examines vulnerabilities across all communication layers from the physical and MAC layers to network routing and application layer message formats thereby establishing the technical foundation for subsequent experimental evaluations.

Building upon this foundation, the research develops a novel three tier testing framework capable of emulating realistic cyberattacks and assessing their impact under controlled yet representative conditions. As detailed in Chapter 4 - 6, this framework integrates:

- SDR platforms (USRP devices with GNU Radio) for controlled physical-layer

attack emulation.

- Industrial-grade Cohda Wireless MK6 equipment for commercial implementation assessment.

- The CyberVehiCare hardware in the loop testbed [18] for intermediate scale validation involving connected vehicles.

This multi tier approach enables systematic experimentation across diverse attack vectors including jamming, message injection, replay, timing manipulation, and Sybil identity spoofing. The framework measures their effects on critical performance metrics such as latency, packet delivery ratio, message integrity, and cooperative awareness reliability, thereby generating empirical data that reflect real world vehicular communication behavior.

The study further enhances vulnerability assessment through the development of machine learning based physical layer security monitoring, described in Chapter 5. Recognizing that traditional cryptographic techniques primarily protect higher-layer communications, this research focuses on lower layer vulnerabilities such as reactive jamming, signal manipulation, and channel state exploitation. A hybrid detection architecture combining Graph Neural Networks (GNNs) with temporal sequence models achieves 97.3% attack detection accuracy while maintaining a 42 ms inference latency demonstrating feasibility for real time vehicular deployment.

Additionally, the research adapts conventional cybersecurity risk assessment methodologies, originally designed for enterprise IT systems, to the specific operational context of V2X networks. Chapter 3 introduces a quantitative risk management framework incorporating V2X-specific metrics such as Safety Impact Score (SIS), Real Time Performance Degradation Factors, and Cooperative Function Impact Indices. These metrics account for the temporal sensitivity, high mobility, and safety-critical nature of vehicular environments, aligning the assessment process with automotive cybersecurity standards including ISO/SAE 21434 [19] and UNECE WP.29 R155/R156 [20].

Together, these elements form a holistic three-tier integration framework that overcomes the limitations of traditional assessment methodologies, which often isolate specific protocol layers or rely solely on simulation. While SDR platforms enable controlled emulation of sophisticated physical and data link layer attacks, large-scale traffic simulation tools (e.g., SUMO, ns3) allow modeling of realistic vehicular topologies involving thousands of nodes. Industrial hardware validation using Cohda Wireless devices ensures that findings generalize to real world deployment scenarios rather than remaining confined to academic prototypes.

By incorporating realistic operational constraints such as relative vehicular velocities exceeding 500 km/h, ultra-low latency requirements ($<$100 ms for safety-critical messages), dynamic spectrum variations, multipath fading, and interference conditions the framework ensures strong alignment with real world deployment scenarios. It explicitly evaluates how protocol layer attacks propagate to compromise system level outcomes, including cooperative awareness degradation, safety application malfunction, and reduced traffic efficiency.

In addition to its experimental rigor, the framework underpins enhanced awareness, research, and training in the V2X sector through hardware in the loop integration using the CyberVehiCare testbed. This capability enables hands-on engagement

with vehicular communication technologies, supporting both academic research and professional training in compliance with ISO/SAE 21434 [19] personnel competence requirements. By bridging experimental research with workforce development, the CyberVehiCare platform fosters a sustainable ecosystem that strengthens industry academia collaboration and accelerates the secure adoption of intelligent transportation technologies.

Consequently, the proposed methodology yields more accurate, scalable, and operationally relevant insights into V2X cybersecurity resilience than traditional single paradigm approaches. It provides a unified foundation for vulnerability discovery, risk quantification, real time detection, and cybersecurity education contributing directly to the development of resilient, reliable, and trustworthy ITS suitable for large scale deployment.

1.5 Contributions of the Study

This research makes five principal contributions advancing both the theoretical understanding and practical implementation of security within V2X communication systems. These contributions address critical gaps in protocol analysis, assessment methodology, experimental validation, physical layer monitoring, and organizational competence collectively providing a systematic framework for V2X cybersecurity that spans technical, operational, and human dimensions.The structure of this Thesis reflects a comprehensive approach to cybersecurity risk management in V2X environments, with each Chapter addressing a specific objective.

First, the research provides comprehensive protocol level security analysis of the three primary communication families underpinning V2X systems: DSRC (IEEE 802.11p), Cellular V2X technologies (LTE V2X and 5G NR V2X) and GNSS, and in-vehicle CAN bus architectures. Chapter 2 delivers systematic examination of security mechanisms, identifies protocol specific vulnerabilities, and characterizes distinct cross protocol attack vectors arising when heterogeneous technologies operate within unified vehicular platforms. This analysis establishes the technical foundation enabling subsequent risk assessment and vulnerability evaluation frameworks.

Second, building upon prior SDR based V2X research [16, 21] and leveraging the CyberVehiCare integrated testbed [18], the thesis develops a novel three tier vulnerability assessment framework integrating SDR emulation, hardware in the loop systems, and industrial V2X equipment validation. Chapter 4 presents systematic evaluation of attack scenarios spanning jamming, message injection, replay attacks, timing manipulation, and identity spoofing, providing empirical data regarding impacts on latency, packet delivery, message integrity, and cooperative awareness. This represents the first integration of SDR based IEEE 802.11p physical layer emulation with intermediate scale testbed validation and commercial Cohda Wireless hardware assessment within a unified experimental framework.

Third, Chapter 3 develops adapted risk management frameworks specifically tailored to V2X cybersecurity requirements, extending traditional IT security methodologies (NIST SP 800 30, ISO/IEC 27005) with novel V2X specific metrics. The framework introduces Safety Impact Scoring, Real time Performance Degradation factors, and Cooperative Function Impact indices that explicitly account for the safety critical nature of vehicular communications. These adaptations align with automotive cybersecurity standards (ISO/SAE 21434) and regulatory requirements

(UNECE WP.29 R155/R156), providing practical risk assessment tools suitable for automotive industry deployment.

Fourth, Chapter 5 extends vulnerability assessment capabilities through development of machine learning based physical layer security monitoring, addressing attack vectors (reactive jamming, signal manipulation, channel state exploitation) that operate below traditional cryptographic protection layers. The research develops hybrid detection architectures combining GNNs with Long Short Term Memory (LSTM) model, achieving 97.3% attack detection accuracy with inference latency suitable for real time vehicular deployment (<50 ms per classification). This contribution enables continuous security monitoring complementing cryptographic message authentication mechanisms.

Fifth, recognizing that technical security measures require organizational competence for effective implementation, Chapter 6 develops a comprehensive cybersecurity awareness and training framework addressing human factors in V2X security. The CyberVehiCare testbed is adapted as a training platform supporting six hands-on modules (CAN bus injection, ECU spoofing, V2X message attacks, jamming, MitM attacks, intrusion detection). Empirical evaluation demonstrates training effectiveness through quantified knowledge gains, exercise completion rates. The framework implements a three tier competence model (Awareness → Training → Education) aligned with ISO/SAE 21434 Clause 5.4.2 personnel competence requirements, providing practical guidance for automotive organizations implementing cybersecurity programs.

Collectively, these contributions span protocol analysis (Chapter 2), risk management frameworks (Chapter 3), experimental validation methodologies (Chapter 4), advanced detection capabilities (Chapter 5), and organizational implementation (Chapter 6), providing a holistic approach to V2X cybersecurity that addresses technical vulnerabilities, operational risks, and human factors within a unified framework suitable for both academic research and industrial deployment.

1.6 Thesis Organization

The remainder of this thesis comprises five chapters that systematically address V2X cybersecurity from protocol level technical analysis through organizational competence frameworks, with each chapter building upon foundations established in prior sections.

Chapter 2: V2X Communication Systems—Protocols and Technologies establishes the technical foundation by providing comprehensive analysis of four protocol families underpinning vehicular connectivity. The chapter examines DSRC based on IEEE 802.11p (including physical layer OFDM characteristics, OCB mode operation, and IEEE 1609.x security services), Cellular V2X technologies encompassing both LTE V2X and 5G NR V2X (analyzing Mode 3 scheduled and Mode 4 autonomous resource allocation), GNSS providing positioning and timing synchronization, and in-vehicle CAN architectures. Security mechanism analysis includes Public Key Infrastructure (PKI) frameworks (IEEE 1609.2, ETSI TS 103 097), pseudonymous certificate management, and misbehavior detection systems. The chapter identifies distinct attack surfaces spanning physical layer (jamming, signal manipulation), medium access control layer (channel access exploitation), network layer (routing attacks), and application layer (message injection, replay

attacks). This technical foundation directly informs the risk assessment frameworks developed in Chapter 3 and experimental attack scenarios evaluated in Chapter 4.

Chapter 3: V2X Cybersecurity Risk Management develops quantitative risk management frameworks adapted specifically for vehicular communication requirements, building upon automotive cybersecurity standards (ISO/SAE 21434) and regulatory mandates (UNECE WP.29 R155/R156). The chapter extends traditional IT risk methodologies (NIST SP 800 30, ISO/IEC 27005) by introducing novel V2X specific metrics including Safety Impact Score (quantifying potential physical harm from communication compromises), Real time Performance Degradation factors (measuring latency and reliability impacts), and Cooperative Function Impact indices (assessing degradation of multi vehicle coordination). Risk assessment methodology incorporates attack taxonomy (jamming, spoofing, Sybil attacks, replay attacks, man in the middle), quantitative analysis techniques (V2X adapted CVSS scoring), and mitigation strategies spanning cryptographic protection, machine learning based intrusion detection, and multi channel redundancy. These frameworks provide theoretical foundations for the practical vulnerability assessment methodologies implemented in Chapter 4, explicitly addressing the inverted security priority structure of V2X systems (availability and integrity over confidentiality) compared to traditional IT environments.

Chapter 4: Security Risk and Vulnerability Assessment for V2X Wireless Networks implements comprehensive experimental validation through multi-testbed architecture, translating the risk frameworks from Chapter 3 into practical assessment methodologies. The chapter describes design and implementation of SDR testbeds using USRP B210 devices with GNU Radio 3.10 flowgraphs for physical layer IEEE 802.11p transceiver emulation and attack generation (jamming, selective message injection, timing manipulation). Industrial validation employs Cohda Wireless MK6 On Board Units and Road Side Units to assess vulnerability assessment methodology generalization to commercial V2X implementations. Experimental results on attack scenarios, quantifying impacts on key performance indicators (latency degradation, packet delivery ratio reduction, message integrity compromise, cooperative awareness disruption) under various traffic densities and attack intensities. Cross tier consistency analysis validates SDR emulation fidelity against industrial hardware behavior, while comparative evaluation demonstrates assessment methodology improvements over conventional single tier approaches.

Chapter 5: Vulnerability Monitoring Technology in Physical Layer Security for C-V2X Communications extends the assessment framework by addressing physical layer security monitoring through machine learning based detection mechanisms. While Chapters 3–4 focus on protocol and system level vulnerabilities addressable through cryptographic protections and testbed assessment, Chapter 5 recognizes that sophisticated attacks targeting physical layer characteristics (reactive jamming, signal level manipulation, channel state exploitation) operate below traditional security mechanisms. The chapter develops hybrid neural network architectures combining GNNs (capturing spatial relationships among vehicular nodes) with LSTM temporal models (detecting anomalous signal patterns over time) to achieve real time attack detection. Experimental validation using the SDR testbed from Chapter 4 demonstrates 97.3% detection accuracy across jamming, spoofing, and signal manipulation attacks, with inference latency below 50 ms suitable for vehicular deployment. Feature fusion techniques integrate RF signal characteristics

(received signal strength, signal to noise ratio, channel state information) with protocol level metrics (packet arrival patterns, message sequence analysis) to enhance detection robustness. This contribution complements cryptographic authentication mechanisms by enabling continuous physical layer security monitoring, addressing the complete V2X protocol stack from physical layer through application layer.

Chapter 6: Cybersecurity Awareness Research and Training in V2X Sector transitions from purely technical security mechanisms to organizational and human factors, recognizing that technological protections require skilled personnel and organizational competence for effective implementation. The chapter addresses regulatory personnel requirements (ISO/SAE 21434 Clause 5.4.2, UNECE R155 Article 7) through development of a comprehensive training and awareness framework. The CyberVehiCare testbed is adapted as a hands-on training platform supporting six experiential modules: CAN bus message injection, Electronic Control Unit spoofing, V2X message attacks, RF jamming, Man-in-the-Middle (MitM) attacks, and Intrusion Detection System (IDS) configuration. Empirical effectiveness evaluation demonstrates quantified learning outcomes sustained knowledge and vulnerability identification improvement. This organizational perspective completes the thesis's holistic approach to V2X cybersecurity, bridging technical vulnerability assessment (Chapters 2–5) with practical automotive industry implementation requirements.

Chapter 7: Conclusions and Future Directions synthesizes the research contributions, explicitly answers the three research questions formulated in Chapter 1, and evaluates the thesis's theoretical and practical implications. The chapter provides systematic synthesis of how protocol analysis (Chapter 2), risk management frameworks (Chapter 3), experimental validation (Chapter 4), physical layer security monitoring (Chapter 5), and organizational competence development (Chapter 6) collectively address the identified gaps in V2X cybersecurity assessment. This progressive structure provides both theoretical rigor and practical guidance for developing secure, resilient V2X communication systems suitable for large scale deployment in safety critical automotive applications. The chapter positions secure V2X communication not as aspirational but as an achievable engineering challenge requiring sustained cross stakeholder collaboration among researchers, manufacturers, regulators, and educators to realize connected vehicles worthy of their profound societal responsibility.

1.7 Conclusion

This introductory chapter has established the foundational context, research framework, and organizational structure for investigating V2X cybersecurity through systematic vulnerability assessment methodologies adapted to the unique requirements of vehicular communication systems. The chapter identified critical gaps in existing assessment approaches specifically the absence of integrated frameworks spanning physical layer emulation, large scale simulation, and industrial validation and positioned this research as addressing these limitations through three tier testbed integration and novel risk management adaptations. The three central research questions guide investigation of protocol heterogeneity challenges, experimental testing requirements, and methodology adaptation needs, while the stated hypothesis proposes that multi tier integration provides superior assessment capabilities compared to conventional single paradigm approaches.

The subsequent chapters build systematically upon this foundation, progressing from technical protocol analysis. Collectively, this research contributes both to academic understanding of V2X security vulnerabilities and to practical deployment guidance for automotive industry stakeholders developing next generation ITS.

Chapter 2

V2X Communication Systems: Protocols and Technologies

2.1 Introduction

The escalating complexity of modern transportation ecosystems necessitates a paradigm shift from isolated vehicular operation toward cooperative, intelligence enhanced mobility systems. Contemporary traffic fatality statistics, that exceed 1.35 million deaths annually worldwide, underscore the critical imperative for transformative communication technologies that transcend traditional automotive safety mechanisms [3]. This chapter contribution examines the foundational communication protocols enabling V2X systems, with particular emphasizing technical architectures, performance characteristics, and interoperability challenges that define next generation Cooperative Intelligent Transportation Systems (C-ITS), with particular attention to protocol characteristics relevant to the cybersecurity analysis in subsequent chapters

This chapter addreses: (a) what are the critical technical trade offs between IEEE-802.11p-based DSRC and 3GPP Cellular V2X (C-V2X) technologies? (b) how do cross stack interoperability challenges between regional implementations (North American WAVE vs. European ITS-G5 vs Asian C-V2X deployments) affect global V2X adoption? (c) what are the fundamental limitations of current security frameworks?

This chapter synthesizes technical specifications from foundational standards bodies (IEEE, ETSI, 3GPP, SAE International) with analysis of performance evaluation methodologies, security vulnerabilities, and deployment challenges. The analytical framework establishes the technological foundation for the cybersecurity risk assessment methodologies presented in subsequent chapters.

2.2 V2X Communication Ecosystem Foundation

The technical foundation of V2X systems rests upon the C-ITS reference architecture defined in ETSI EN 302 6655 [2], with four distinct station types with specialized functional responsibilities. The Vehicle ITS Station(V-ITS-S) architecture encompasses On Board Units (OBUs) integrated with sensor arrays, Electronic Control Units (ECUs), and CAN bus infrastructure. Contemporary implementa-

tions incorporate multi constellation GNSS receivers, Inertial Measurement Units (IMUs), and vehicular radar/lidar systems to enable centimeter level positioning accuracy required for advanced cooperative applications [22, 23] as shown in Figure 2.1. Several major automotive manufacturers have already announced timelines for the deployment of fully autonomous connected vehicles capable of independent operation [24]. Critical performance parameters include position update rates (1-10 Hz), CAM generation latency (<100 ms), and integrated security processing support pseudonymous authentication [25, 26].

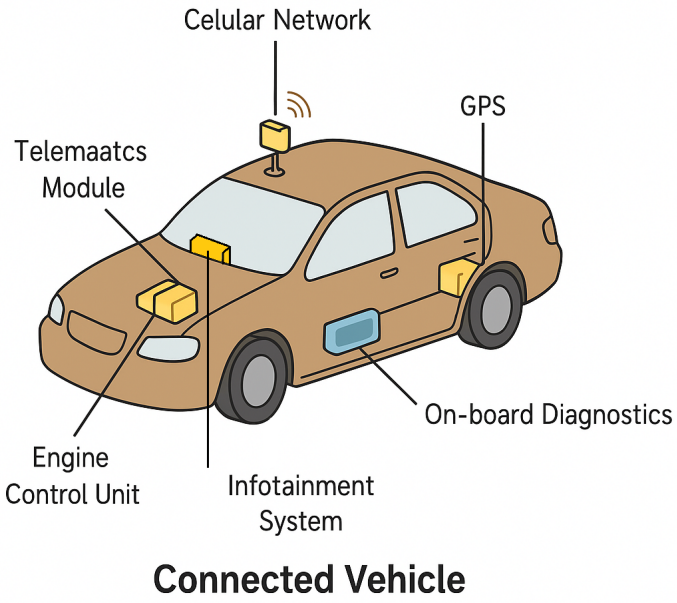


Figure 2.1: Autonomous Connected vehicle equipped with sensors for decision making while driving

However, realizing this vision depends on a reliable and robust communication infrastructure as ITS integrate communication, sensing, and data processing technologies into vehicles, roadside infrastructure, and user interfaces. The systems operate within a heterogeneous network, divided into two primary sub networks [27], as illustrated in Figure 2.2.

The intra vehicle network uses standardized automotive protocols such as CAN[28], LIN[29], FlexRay[30], and Automotive Ethernet[31]. Modern vehicles may also integrate Wi-Fi for infotainment system connectivity and diagnostic interfaces. In contrast, the inter vehicle network enables communication between the vehicle and external devices in its surroundings. Figure 2.2 illustrates V2X Communication Ecosystem Architecture showing C-ITS station types, communication modes, and technology integration across vehicular, infrastructure, personal, and central domains. The diagram illustrates bidirectional communication flows, spectrum utilization, and performance characteristics for IEEE-802.11p, LTE-V2X, and 5G NR-V2X technologies. This network is structured around four main entities which are described as follows.

- On-Board Units (OBUs) are fundamental components of ITS. Each vehicle is equipped with an OBU that processes locally collected data and enables

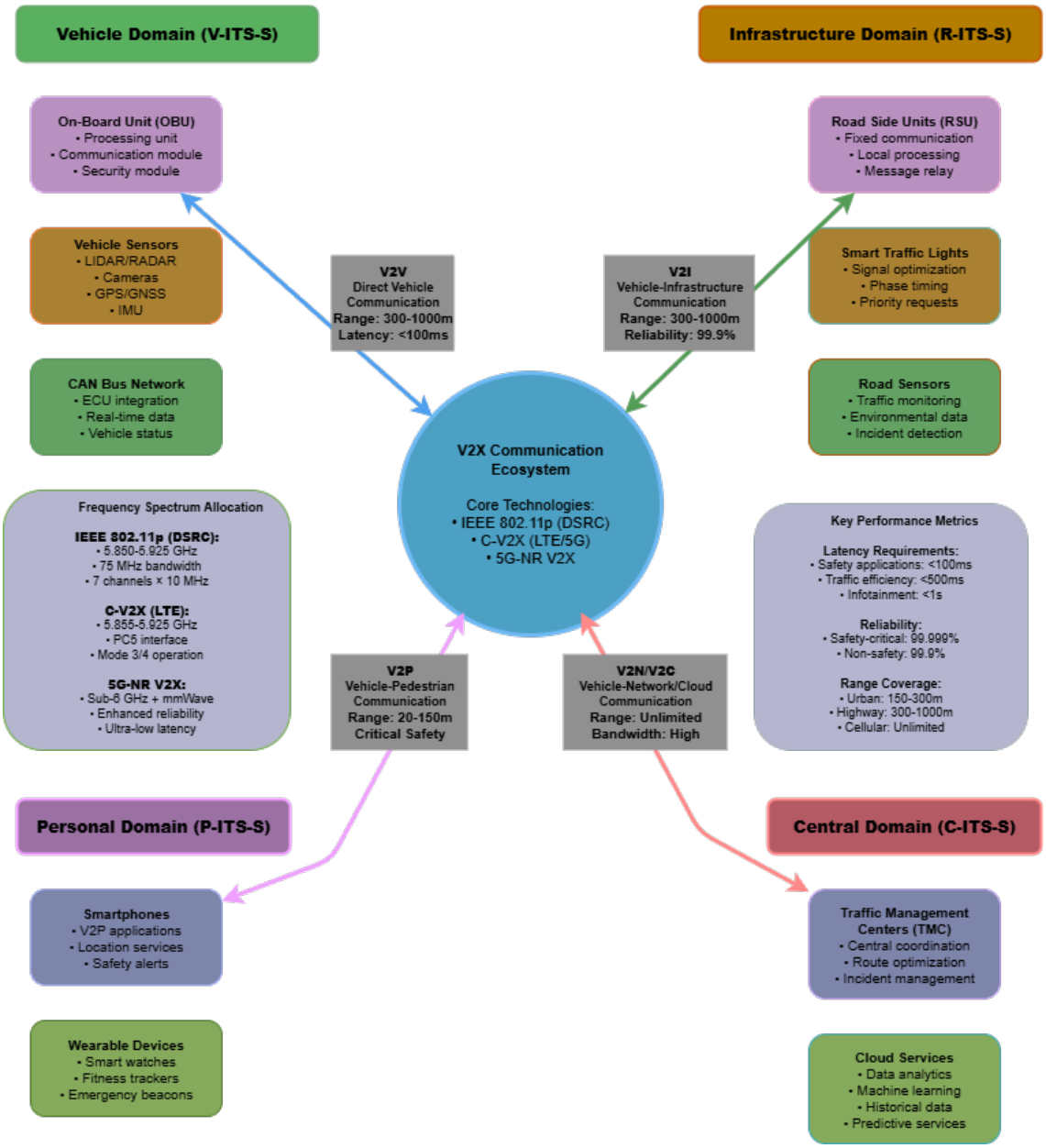


Figure 2.2: V2X Communication Ecosystem Architecture

interaction with surrounding entities and networks. Acting as the vehicle's communication and computation hub, the OBU supports real time information exchange and both safety- and efficiency-oriented applications.

- Personal ITS Stations (P-ITS-S) address Vulnerable Road User (VRU) protection through smartphone-based applications, dedicated wearable devices, and integrated public transportation systems. Key challenges include energy efficiency, communication handover, and privacy preservation. These mechanisms must ensure anonymity while supporting safety-critical messaging [32].

- Roadside ITS Stations (R-ITS-S) are fixed infrastructure elements strategically positioned to extend communication coverage, provide local traffic management services, and serving as edge computing platforms for latency sensitive applications [27] with compatibility for direct PC5 sidelink communication and network assisted V2N connectivity [33, 34].

- Central ITS Stations (C-ITS-S) provide system wide coordination through Traffic Management Centers (TMCs), cloud-based analytics platforms, and distributed edge computing infrastructure. They support large scale data aggregation, and response to traffic incidents or security events. Integration with 5G network slicing allows dedicated V2X service provisioning with guaranteed Quality of Service (QoS) parameters [35, 36]. Through centralized control, the server improves system-wide efficiency, enhances decision-making, and enables services such as traffic prediction, route optimization, and smart city integration.

The communication taxonomy encompasses four primary interaction modes, each characterized by distinct performance requirements and technical challenges [37]. Figure 2.3 illustrates various scenarios within a V2X network, wherein VUEs (connected vehicle) interact with diverse infrastructure elements, including RSUs, traffic lights, public parking areas, road signs, and smart road communication units. Communication between different V2X entities requires the integration of numerous sensors, communication devices, and technologies, leading to the generation of significant data communication messages [33, 34]. This enables a wide spectrum of applications, ranging from safety to traffic management and infotainment services [38].

These messages can be broadly distinguished according to their purpose and communication scope. V2V communication enables direct peer to peer information exchange without infrastructure dependency, critical for collision avoidance and cooperative awareness applications. V2I facilitates interaction with roadside systems, traffic management platforms, and fixed sensors. V2P addresses VRU protection through direct communication with personal devices. V2N/V2C enables access to cloud-based services, over the air software updates, and wide area traffic coordination [39, 40].

Performance analysis reveals fundamental trade offs between communication range, latency, reliability, and spectrum efficiency that influence technology selection for specific application scenarios. Direct V2V communication achieves ultra low latencies ($<$10 ms) essential for collision avoidance but operates within limited range constraints (300-1000 m). Network assisted V2N communication provides extended coverage and higher data throughput but introduces additional latency through cellular infrastructure processing [41].

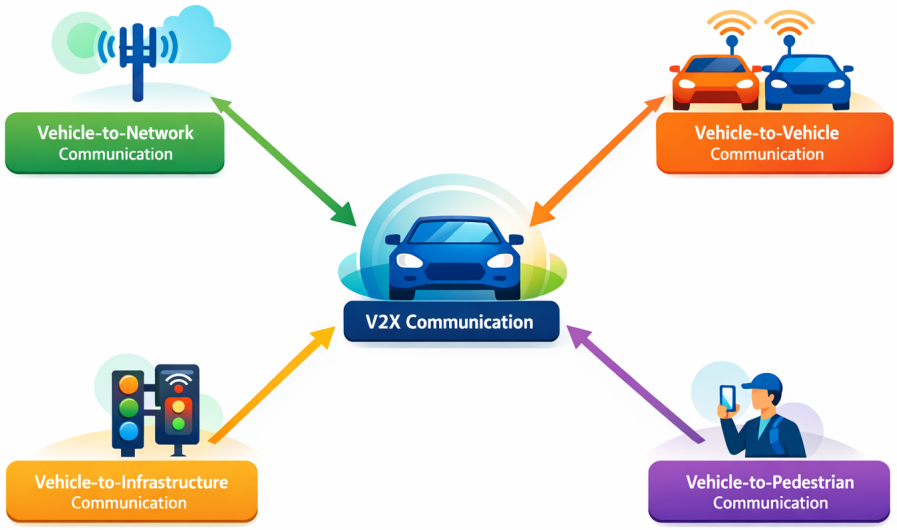


Figure 2.3: Architecture of Vehicle to Everything (V2X) [1]

2.3 Access Technologies and Physical Layer Analysis

The evolution of V2X access technologies reflects a progression from purpose built vehicular communication systems toward integration with broader cellular communication infrastructure. This section provides critical analysis of the three dominant technology families, examining their technical architectures, performance characteristics, and deployment implications through standardized evaluation methodologies. Figure 2.4 provides a comparative analysis of V2X access technologies, showing the performance envelopes for IEEE-802.11p, LTE-V2X, and 5G NR-V2X across latency, reliability, range, and data rate dimensions. The diagram includes a technology evolution timeline from 2010 to 2025, quantitative performance metrics-based on 3GPP specifications, and field testing on standardized evaluation methodologies.

2.3.1 IEEE-802.11p/DSRC Systems Architecture

DSRC provides low latency, highly reliable communication between V2V and V2I and is based on IEEE-802.11p [8, 42] standard using 10 MHz Orthogonal Frequency Division Multiplexing (OFDM). The IEEE-802.11p physical layer employs a 64 point Fast Fourier Transform (FFT) with 52 active subcarriers (48 data, 4 pilots) and 8 μs symbol duration to mitigate Doppler effects [34, 43]. Modulation schemes range from Binary Phase Shift Keying (BPSK) to 64 Quadrature Amplitude Modulation (QAM) to achieve data rates between 3 and 27 Mbps over 10 MHz channels. Performance analysis indicates that MCS 0 (BPSK, rate 1/2) offers maximum range and reliability for safety critical applications. DSRC operates in Outside the Context of a Basic Service Set (OCB) mode, bypassing conventional Wi-Fi association to allow immediate transmission. At the MAC layer, Enhanced Distributed Channel Access (EDCA) enables QoS differentiation through four Access Categories: Voice (AC_VO), Video (AC_VI), Best Effort (AC_BE), and Background (AC_BK), each

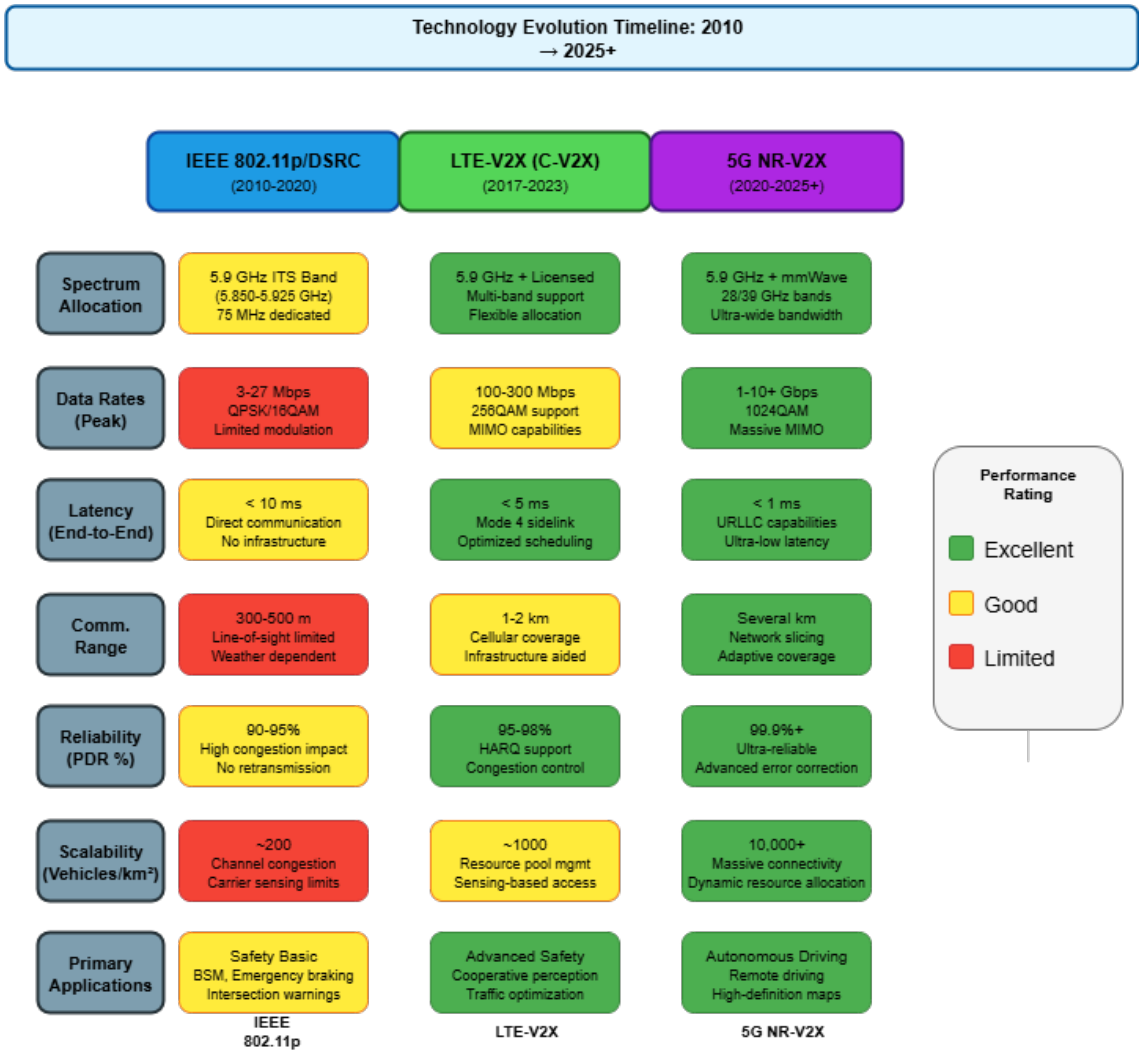


Figure 2.4: A comparative analysis of V2X access technologies

defined by distinct Arbitration Interframe Space (AIFS) and Contention Window parameters [44].

Operating in the 5.875–5.925 GHz ITS band, DSRC defines seven 10 MHz channels: one Control Channel (CCH 178) and six Service Channels (SCH 172, 174, 176, 180, 182, 184) [45]. This configuration ensures that messages are disseminated efficiently and reliably to all vehicles within range, supporting rapid situational awareness and timely hazard response. DSRC supports safety critical information with latencies below 100 ms. In North America, vehicles transmit SAE J2735 [46] Basic Safety Messages (BSMs), which include Part I core data and optional Part II extensions for enhanced situational awareness [43]. European implementations uses ETSI CAMs and DENMs for event triggered hazard notifications such as accidents, roadwork, or emergency situations [44]. Figure 2.5 DSRC-based V2X communications architecture. This frequent exchange of status information allows vehicles and roadside units to maintain an accurate, real time model of their surrounding environment. By enabling proactive awareness and reactive hazard response, these messages form the backbone of C-ITS.

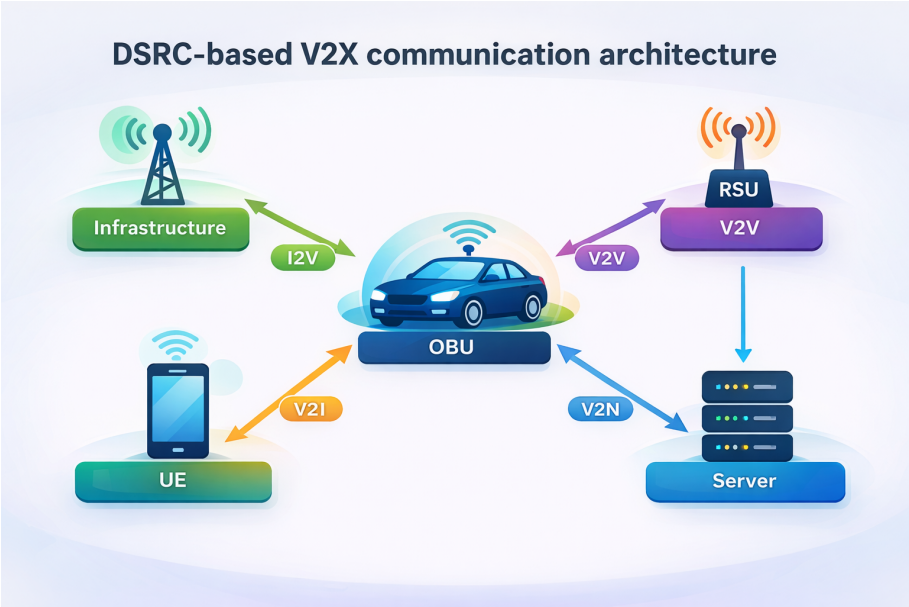


Figure 2.5: DSRC-based V2X communications architecture

Despite its advantages, DSRC faces limitations. Its effective range is between 300 m and 1 km, which, while sufficient for immediate safety applications, may not meet the demands of wide area services. High density traffic causes channel congestion, particularly when the Channel Busy Ratio (CBR) exceeds 0.6 [47]. DCC mitigates these effects through adaptive transmission rate, power, and data rate control.

Regulatory challenges constrain DSRC deployment. Portions of the 5.9 GHz spectrum have been reallocated for unlicensed Wi-Fi use. In the United States, the FCC reassigned the upper 45 MHz (5.895–5.925 GHz) for unlicensed use, leaving only 30 MHz (5.850–5.895 GHz) dedicated to vehicular safety applications [48].

2.3.2 Cellular V2X Technologies (LTE-V2X and 5G NR-V2X)

Cellular V2X [49, 50] employs scheduled resource allocation optimized for vehicular communication requirements. LTE-V2X [51], standardized in 3GPP Release 14/15,

introduces PC5 sidelink [52], enabling direct V2V and V2I communication without cellular networks dependency and Uu interface compatibility for V2N services requiring cloud support or wide area coverage [53] as shown in Figure 2.6.

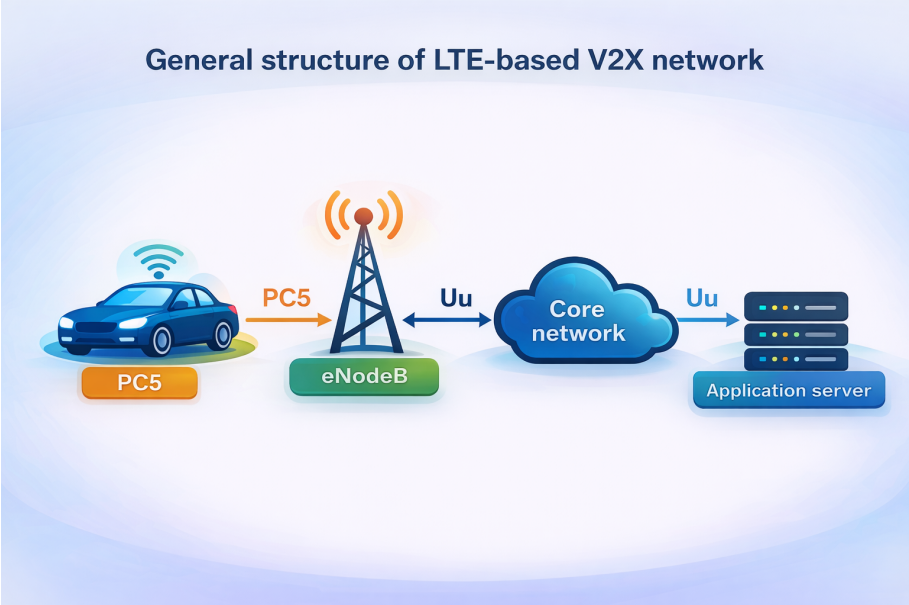


Figure 2.6: General architecture of C-V2X network

LTE-V2X implements two resource allocation modes. Mode-3 employs evolved NodeB (eNB) scheduling, providing centralized resource allocation with optimized interference management suitable for managed infrastructure deployments. Mode-4 utilizes Semi Persistent Scheduling (SPS)-based on distributed sensing, enabling autonomous sidelink operation in coverage limited environments [54] as shown in Figure 2.7. The SPS mechanism allows vehicles to autonomously select transmission resources based on channel sensing, with configurable periodicity (20, 50, 100, 200, 500, 1000 ms) adapted to application requirements [55, 56]. Resource pool based allocation provides predictable performance, with PDR maintaining >95%, under high vehicle density conditions.

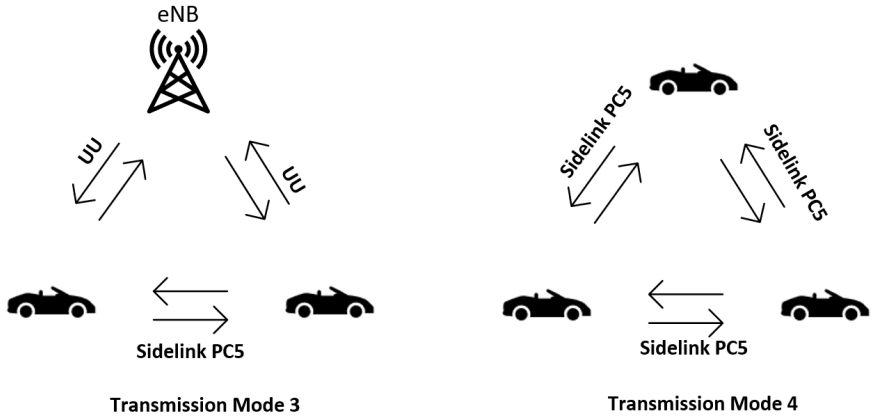


Figure 2.7: Transmission modes of V2X

5G New Radio V2X (NR-V2X) addresses requirements of autonomous driving applications through Ultra Reliable Low Latency Communication (URLLC) [57].

Target performance specifications include sub 1 ms latencies for critical safety applications, multi gigabit data rates for cooperative perception, and 99.999% reliability for mission critical communications.

NR-V2X supports including unicast, groupcast, and broadcast communication modes. Enhanced Hybrid Automatic Repeat Request (HARQ) feedback enabled reliable communication in radio environments [58, 59]. Integration with 5G System (5GS) facilitates network slicing for differentiated V2X service provisioning and Multi Access Edge Computing (MEC) for ultra low latency applications [36].

2.3.3 Physical Layer Parameters and Performance Analysis

IEEE-802.11p operates exclusively in the 5.9 GHz ITS band with fixed 10 MHz channelization, providing deterministic spectrum access but limited flexibility for varying bandwidth requirements [45]. LTE-V2X supports operation in both dedicated ITS spectrum and cellular bands, enabling flexible spectrum utilization and coexistence with existing cellular services [60].

Table 2.1: Comparative Physical Layer Parameters for V2X Access Technologies

Parameter	**IEEE-802.11p**	**LTE-V2X**	**5G NR-V2X**
Spectrum	5.9 GHz ITS band	5.9 GHz + cellular	Flexible 5G NR bands
Channel Bandwidth	10 MHz fixed	10/20 MHz	Variable (100-400 MHz)
Modulation	BPSK to 64 QAM	QPSK to 64 QAM	QPSK to 256 QAM
Access Method	CSMA/CA	Resource pools	Advanced scheduling
Latency	<10 ms	10-20 ms	<1 ms (URLLC)
Range	300-500 m	Up to several km	Enhanced coverage
Data Rate	3 Mb/s – 27 Mb/s (per 10 MHz channel)	3 Mb/s – 80 Mb/s(Higher than 802.11p)	Multi Gbps potential
Reliability	95% PDR (ideal)	>95% (congested)	99.999% (URLLC)

Table 2.1 shows that IEEE-802.11p achieves low latencies (<10 ms) for single hop broadcast communication, making it optimal for collision avoidance and emergency braking applications. LTE-V2X Mode-4 exhibits 10-20 ms latencies depending on SPS configuration and traffic loading, while Mode-3 may introduce additional delays through eNB scheduling processes. New Radio V2X Ultra Reliable Low Latency Communication (NR-V2X URLLC) targets sub millisecond latencies for advanced applications, such as cooperative perception and coordinated automated driving.

IEEE-802.11p provides performance within 300-500m range. LTE-V2X achieved multi kilometer range. NR-V2X incorporates advanced antenna technologies including massive MIMO and beamforming to further enhance coverage and spectral efficiency.

Reliability analysis shows that IEEE-802.11p provides deterministic performance under low density but suffers from collision induced packet loss as vehicle density increases. LTE-V2X resource pool allocation provides consistent reliability across varying density conditions. NR-V2X URLLC mechanisms target 99.999% reliability

for mission critical applications through advanced error correction and diversity techniques [49].

2.3.4 Comparative Technology Assessment

Critical technology assessment reveals that optimal V2X deployments will likely employ hybrid approaches leveraging the complementary strengths of different access technologies. IEEE-802.11p excels in latency critical, short range applications where deterministic medium access provides predictable performance. C-V2X technologies offer superior scalability, extended coverage, and integration with existing telecommunications infrastructure.

IEEE-802.11p requires dedicated roadside infrastructure for extended coverage, while LTE-V2X can leverage existing cellular tower infrastructure. NR-V2X deployment demands comprehensive network upgrades but enables integration with 5G services and applications beyond transportation. Interoperability challenges emerge from architectural differences between technologies. While security frameworks (IEEE 1609.2 [61], ETSI TS 103 097 [62]) maintain technology agnostic design, cross technology handover remains limited. Regional deployment variations (North American WAVE, European ITS-G5, and Asian C-V2X) exhibits limited cross compatibility [63, 64]. Future technology evolution toward IEEE 802.11bd (Next Generation V2X) [65] and 3GPP Release 18+ NR-V2X promises enhanced performance and interoperability. However, the transition period will require careful management of legacy system compatibility and cross technology coexistence mechanisms.

2.4 Protocol Stack Architecture and Implementation

V2X protocol stacks adapts traditional networking models to address the requirements of high mobility, broadcast centric vehicular environments. This section examines three protocol families IEEE 1609 WAVE [66], ETSI ITS G5 [44], and 3GPP C-V2X [9] with their architectural differences, interoperability characteristics, and performance implications, as illustrated in Figure 2.8.

2.4.1 WAVE Protocol Stack (IEEE 1609.x Series)

The Wireless Access in Vehicular Environments (WAVE) protocol suite, standardized through the IEEE 1609.x series [67] supports North American V2X deployments. IEEE 1609.3 [11] defines dual networking: the WAVE Short Message Protocol (WSMP) for safety messaging, and IPv6 over IEEE 802.11 OCB for IP-based applications [68]. WSMP operation directly above the IEEE-802.11p MAC layer [42] eliminates IP protocol overhead, utilizing Provider Service Identifiers (PSIDs) for application differentiation rather than traditional port-based addressing. This reduces protocol overhead by approximately 28 bytes per packet compared to IPv6/UDP encapsulation, critical for maintaining latency budgets in safety applications. WSMP supports single hop broadcast for immediate safety messaging and store and forward mechanisms for extended coverage applications. IEEE 1609.4 multi channel coordination introduces temporal separation between Control Channel (CCH) and Service

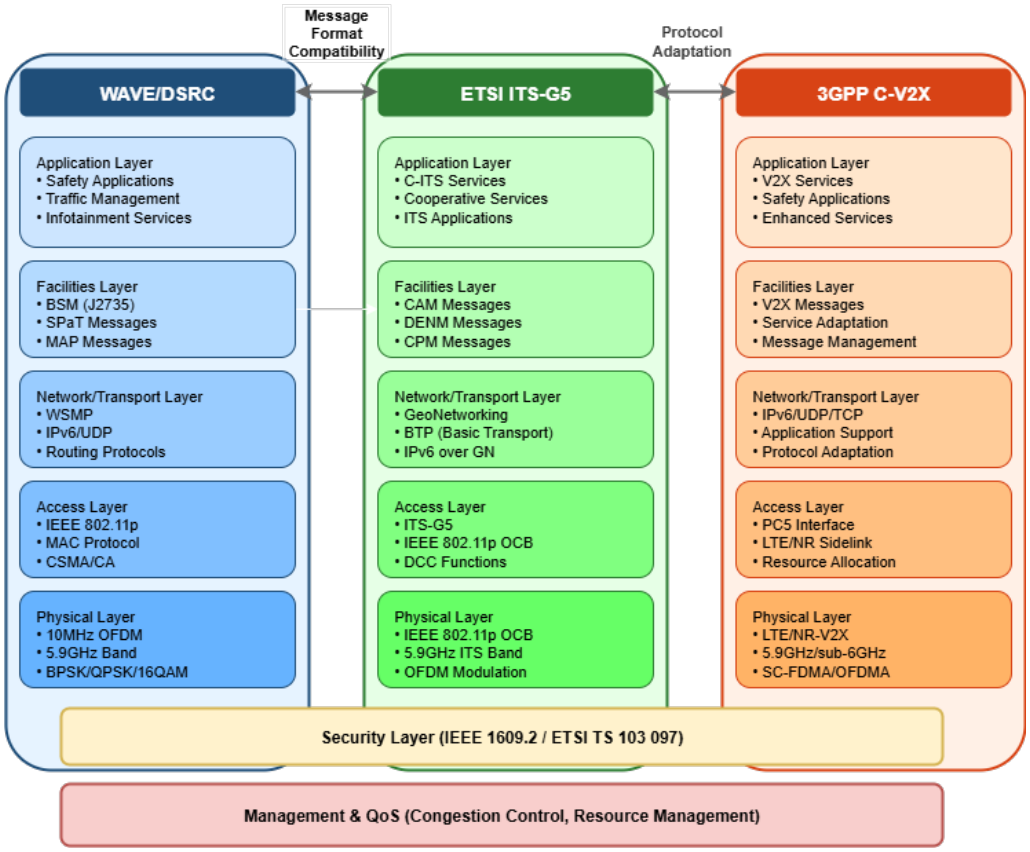


Figure 2.8: Protocol Stack Architecture Comparison

Channel (SCH) operations through 100 ms Synchronization Intervals [12]. The standard specifies alternating 50 ms periods with 4 ms guard intervals accommodating radio retuning latency. During CCH intervals, vehicles must monitor for CAMs and emergency notifications, while SCH intervals support higher bandwidth applications including traffic management and infotainment services. Performance analysis reveals that single radio implementations experience channel switching penalties, with applications suffering periodic service interruptions during CCH monitoring periods. Dual radio architectures eliminate these limitations by enabling simultaneous CCH monitoring and SCH data communication, but require increased hardware complexity and power consumption [12, 12, 34]. WAVE Service Advertisements (WSAs) broadcast on the CCH announce available services and their associated SCH parameters. This discovery mechanism enables dynamic service access but introduces additional protocol overhead and potential scalability limitations in high density scenarios where WSA message collision probability increases significantly [69].

2.4.2 ETSI ITS G5 Protocol Implementation

ETSI ITS G5 [65] protocol architecture adopts a more flexible approach emphasizing media independent upper layer protocols. GeoNetworking (EN 302 636 4 1) provides geographic addressing and forwarding capabilities spanning single hop broadcast, GeoBroadcast, and GeoUnicast communication modes [70]. This approach enables location-based service discovery and message dissemination without requiring traditional routing protocols. The Basic Transport Protocol (BTP, EN 302 636 5 1) [69]

offers connectionless multiplexing through Type A interactive ports and Type B non interactive ports. Well known BTP ports registered in ETSI TS 103 248 [70] enable standardized application identification, while ITS Application Identifiers (ITS AIDs) managed in ETSI TS 102 965 [71] provide security context binding.

GeoNetworking implements sophisticated forwarding algorithms including greedy forwarding and contention-based forwarding for multi hop message dissemination. Location Service (LS) mechanisms enable position-based addressing even when direct geographic coordinates are unavailable. These capabilities prove particularly valuable in sparse network conditions where traditional connected routing fails. IPv6 integration through GN6ASL (TS 102 636 6 1) [69] enables seamless connectivity with IP-based backend systems and cloud services. This dual stack approach provides flexibility for applications requiring both local V2X communication and wide area Internet connectivity.

Critical analysis reveals that GeoNetworking's position dependent forwarding mechanisms require accurate position information and neighbor discovery. Performance degrades significantly when GNSS accuracy is compromised or when vehicles operate in environments with limited positioning infrastructure [69]. The protocol's geographic assumptions also limit applicability in non vehicular ITS applications.

2.4.3 3GPP C-V2X Protocol Architecture

3GPP C-V2X protocol architecture integrates V2X communication capabilities with existing cellular network infrastructure through dual interface design. The PC5 sidelink interface enables direct V2V communication compatible with both LTE-V2X and NR-V2X implementations, as shown in Figure 2.7, while the Uu interface provides network assisted services through cellular base stations [48]. PC5 interface protocols implement comprehensive QoS mechanisms through 5G QoS Identifiers (5QI) and PC5 QoS flows. This enables differentiated service provisioning for varying V2X applications, from basic safety messaging requiring ultra low latency to high bandwidth cooperative perception applications [59]. Advanced HARQ feedback mechanisms provide enhanced reliability compared to broadcast only IEEE-802.11p implementations [72]. 5G System (5GS) integration enables sophisticated network slicing for dedicated V2X service provisioning. Network slices can guarantee specific performance characteristics including latency, throughput, and reliability for different application classes [49]. MEC integration positions compute resources at network edges, enabling ultra low latency processing for time sensitive applications [73]. V2X Application Server (V2X AS) architecture provides centralized application logic and coordination services. This enables complex multi vehicle coordination algorithms, traffic optimization services, and integration with traffic management systems. However, this architecture introduces potential single points of failure and may create scalability challenges in large scale deployments. The 3GPP architecture's cellular [74, 75] heritage provides inherent support for mobility management, authentication and billing systems. This complexity may introduce performance penalties for simple safety applications that could operate more efficiently through direct broadcast mechanisms.

2.4.4 Cross Stack Interoperability Analysis

Cross stack interoperability represents one of the most significant challenges facing global V2X deployment. While security frameworks maintain technology agnostic message formats, fundamental architectural differences create substantial interoperability barriers. Message semantics vary between regional implementations: North American BSM (SAE J2735), European CAM/DENM (ETSI TS 102 637), and Asian implementations exhibit incompatible data structures and transmission patterns [43, 76].Protocol translation mechanisms have been proposed to bridge these differences, but introduce additional latency and complexity that may compromise safety critical application performance. Gateway architectures employing dual stack implementations can provide limited interoperability but require careful management of timing synchronization and message prioritization across different protocol stacks.

Security interoperability presents additional complexity. While IEEE 1609.2 [77] and ETSI TS 103 097 [78] maintain compatible cryptographic mechanisms, certificate management and revocation procedures differ significantly between North American SCMS and European PKI implementations. Cross border vehicle operation requires complex certificate recognition and trust relationship management.Future standardization efforts toward ISO 21177 ITS message harmonization and collaborative security framework development may address some interoperability challenges. However, existing deployments and regulatory differences will likely maintain regional fragmentation for the foreseeable future, requiring hybrid architectures supporting multiple protocol families within individual vehicle platforms [64, 79].

2.5 Multi Channel Coordination and Resource Management

Efficient spectrum utilization and resource management represent critical challenges in V2X systems where safety critical and non safety applications must coexist within limited spectrum allocations. This section examines the technical mechanisms enabling multi channel coordination, congestion control, and resource allocation across different V2X technology families.

2.5.1 IEEE 1609.4 Multi Channel Operation

IEEE 1609.4 multi channel coordination addresses the fundamental challenge of separating safety critical communication from bandwidth intensive applications within shared spectrum resources. The standard defines temporal coordination through 100 ms Synchronization Intervals partitioned into CCH and Service Channel (SCH) periods, nominally allocated as 50 ms each with intervening guard intervals [12]. Critical timing analysis reveals that guard interval duration must accommodate radio retuning latency, crystal oscillator settling time, and synchronization uncertainty across the network. Typical implementations employ 2-4 ms guard intervals, representing 2-4% spectrum efficiency overhead. Single radio implementations must time multiplex CCH/SCH access, creating periodic service interruptions that may affect QOS for continuous applications. Channel coordination policies defined in IEEE 1609.4 [12] include alternating access (mandatory CCH monitoring), continuous access (SCH only operation), immediate access (priority based channel selection),

and extended access (longer SCH intervals) and Policy selection significantly affects both safety message delivery probability and service channel throughput, requiring careful optimization based on application requirements and traffic density. This is shown in Figure 2.9, where Multi Channel Coordination Timing Diagram illustrates IEEE 1609.4 [12] synchronization intervals, Control Channel/Service Channel alternation, guard periods, and performance implications for single radio versus dual radio implementations. The diagram shows message scheduling, channel switching latency, and optimization strategies.

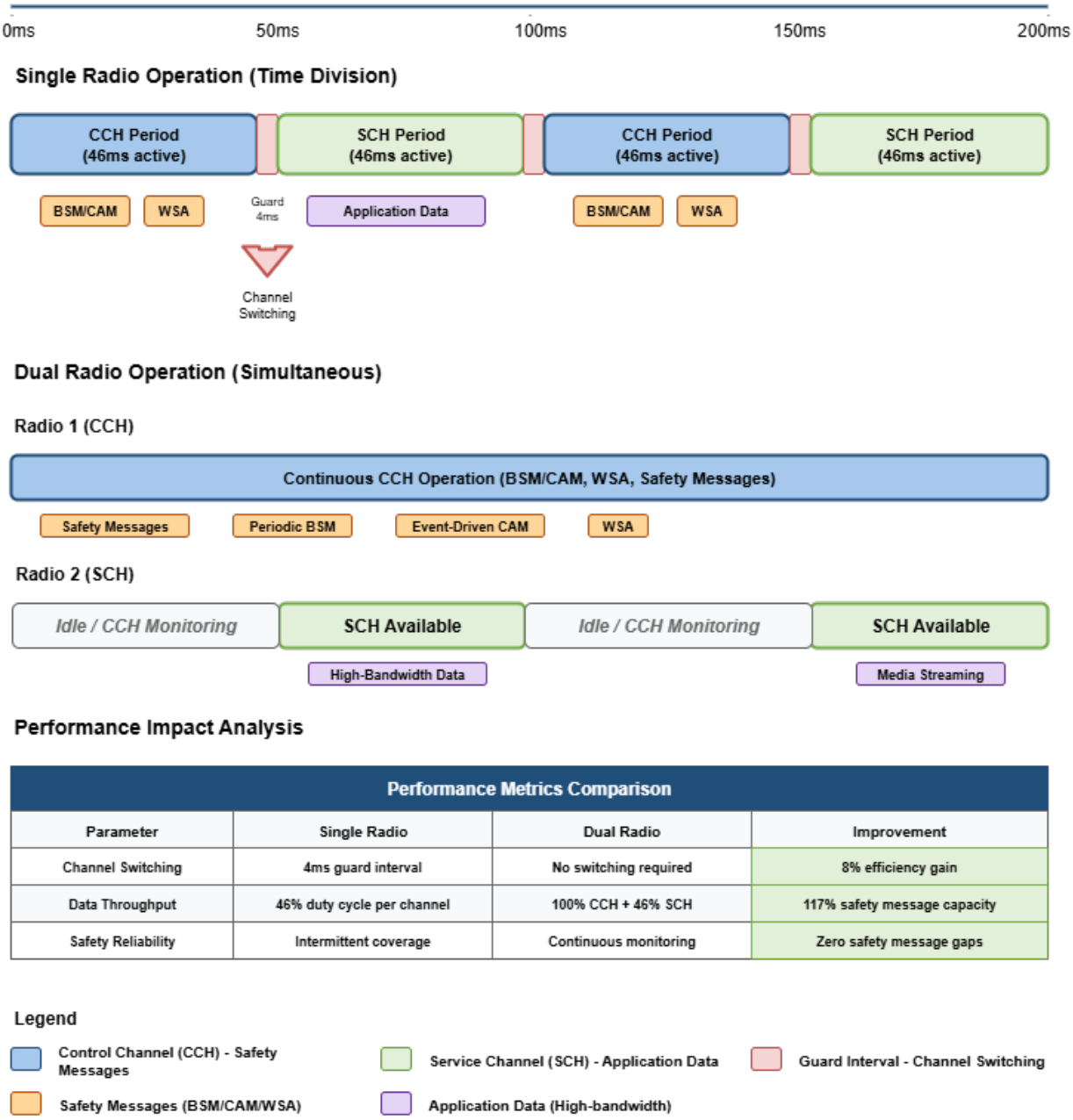


Figure 2.9: Multi Channel Coordination Timing framework

Performance evaluations conducted under standardized conditions, including those defined by IEEE 1609.4 [12] for multi-channel operations and ETSI EN 302 571 [80] for ITS-G5 spectrum access [65], indicate that multi channel coordination in-

troduces substantial system complexity without delivering proportional performance improvements in most deployment scenarios. Safety critical applications primarily demand consistent and deterministic channel access to ensure reliable dissemination of CAM and DENM, rather than maximizing raw bandwidth utilization. In contrast, non-safety or infotainment oriented applications generally exhibit higher tolerance for periodic interruptions and variable latency, making strict multi channel synchronization unnecessary. As a result, emerging approaches, such as dedicated safety channels, context aware channel selection, and dynamic spectrum access mechanisms, have shown promising potential to enhance spectral efficiency, reduce contention, and maintain QoS across heterogeneous vehicular communication environments. These strategies offer a more scalable and operationally efficient alternative to conventional multi channel coordination, particularly under high mobility and dense network conditions typical of large scale V2X deployments.

2.5.2 DCC mechanisms

The ETSI DCC framework provides adaptive resource allocation mechanisms designed to preserve system stability as vehicular density increases. DCC algorithms continuously monitor CBR as the primary congestion indicator, employing reactive feedback control loops to dynamically adjust key transmission parameters, namely Transmit Rate Control (TRC), Transmit Power Control (TPC), and Transmit Data Rate Control (TDC) [47].

The DCC state machine implements three operational states: Relaxed (CBR $<$ 0.3), Active ($0.3 \leq$ CBR < 0.7), and Restrictive (CBR ≥ 0.7), as illustrated in Figure 2.10. State transitions trigger parameter adjustments designed to reduce channel occupation while maintaining essential safety communication. TRC mechanisms reduce CAM generation frequency from 1 to 10 Hz-based on vehicle dynamics and channel conditions [55]. Transitions between these states trigger adaptive parameter reconfigurations designed to balance channel utilization and communication reliability. In the Relaxed state, vehicles employ maximum transmit power, high message generation rates (up to 10 Hz), and optimal data rates to maintain high awareness. As congestion increases, the system transitions to the Active state, applying moderate adjustments in power and rate to sustain performance while avoiding excessive channel occupancy. Under Restrictive conditions, DCC minimizes transmit power, reduces transmission frequency (down to 1 Hz), and selects robust, lower data rates to preserve essential safety communications [55, 56].

Figure 2.10 further depicts how DCC integrates multiple functional components supporting adaptive operation. CBR measurement modules estimate congestion using energy detection and moving average filters. TRC modules regulate message generation frequency and scheduling priority, while TPC algorithms perform dynamic power adjustment to mitigate interference and optimize spatial reuse. TDC mechanisms handle Modulation and Coding Scheme (MCS) selection-based on real-time channel quality indicators, such as RSSI, SINR, and packet error rates. Additionally, auxiliary modules, including sensing-based scheduling, interference management, and resource pool allocation, enable coordinated access to shared radio resources. The lower part of Figure 2.10 illustrates the relationship between throughput and vehicle density, comparing IEEE 802.11p with DCC and LTE-V2X Mode 4 congestion control. The results indicate that both controlled systems outperform unconstrained

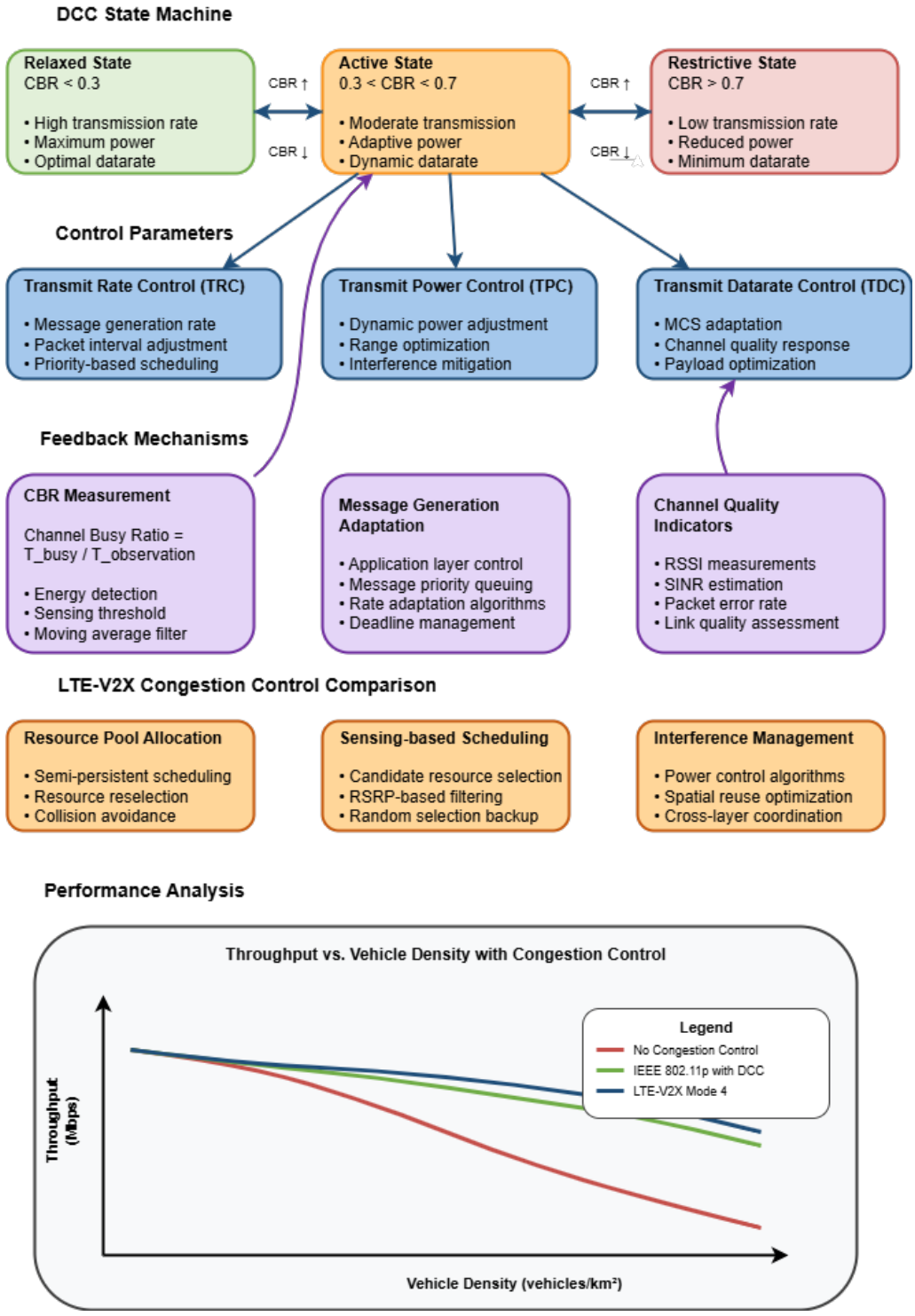


Figure 2.10: DCC state machine showing transitions between Relaxed, Active and Restrictive states

transmission by maintaining higher throughput as density increases, validating DCC's congestion mitigation benefits.

Despite these advantages, critical analysis reveals fundamental limitations in DCC's reactive design. The control loops operate on timescales of several hundred milliseconds, which may be too slow to respond effectively to rapid congestion fluctuations in high mobility environments. DCC inherently assumes cooperative behavior among all participants, rendering the system vulnerable to non compliant or malicious nodes that disregard congestion control policies potentially leading to channel monopolization or DoS conditions.

Empirical evaluations demonstrate that DCC can effectively maintain channel stability under moderate congestion levels, but performance degrades under ultra dense vehicular conditions projected for future autonomous mobility scenarios. To address these challenges, next-generation congestion control approaches, including predictive control models, Machine Learning (ML)-based adaptation, and QoS aware resource allocation mechanisms, are being investigated to enhance responsiveness, fairness, and scalability in future V2X deployments [81].

2.5.3 Resource Allocation in C-V2X

C-V2X resource allocation mechanisms represent a fundamental departure from contention-based IEEE-802.11p approaches toward scheduled access optimized for predictable performance characteristics. LTE-V2X Mode 3 employs evolved NodeB (eNB) centralized scheduling, enabling optimal resource allocation with complete interference coordination. However, this approach requires ubiquitous cellular coverage and may introduce latency through base station processing [82]. Mode 4 Semi Persistent Scheduling (SPS) enables distributed operation suitable for coverage limited scenarios. Vehicles autonomously select transmission resources from configured pools-based on channel sensing and traffic pattern prediction. SPS resource selection algorithms consider historical resource utilization, RSRP measurements from other transmissions, and configurable resource reservation patterns [83]. NR-V2X extends resource allocation capabilities through enhanced grant-based and grant free mechanisms. Grant-based allocation enables precise QoS control for specific applications, while grant free access supports ultra low latency applications that cannot tolerate scheduling delays. Advanced HARQ feedback mechanisms provide reliability enhancement unavailable in broadcast only IEEE-802.11p systems [84].

5G network slicing enables dedicated resource allocation for V2X services with guaranteed performance characteristics. Network slice instances can provide isolated resources with specific latency, throughput, and reliability guarantees tailored to different V2X application requirements [35, 36]. However, slice orchestration complexity and resource efficiency optimization present ongoing challenges. Edge computing integration positions processing capabilities at cellular network edges, enabling ultra low latency applications through reduced propagation delays. MEC platforms can host V2X application servers, traffic coordination algorithms, and real time data processing services. This architecture enables sophisticated cooperative applications, but introduces potential scalability and reliability challenges [73].

2.5.4 Performance Optimization Strategies

Advanced performance optimization strategies for V2X systems encompass cross layer optimization techniques, ML enhanced resource allocation, and hybrid technology approaches. Cross layer optimization enables coordination between physical layer parameters, MAC layer scheduling, and application layer requirements to achieve optimal system performance. Adaptive modulation and coding scheme selection-based on real time channel quality measurements can optimize the trade off between range, reliability, and throughput. Dynamic power control algorithms considering both local channel conditions and network wide interference minimize energy consumption while maintaining communication quality.

ML approaches show promise for predictive resource allocation and congestion control. Reinforcement learning algorithms can optimize resource allocation decisions-based on historical traffic patterns, vehicle mobility predictions, and application requirements. However, the computational complexity and training data requirements may limit practical implementation in resource constrained vehicular environments. Hybrid technology deployment strategies leverage the complementary strengths of different V2X technologies. IEEE 802.11p can provide ultra low latency for immediate safety applications, while C-V2X enables extended coverage and high bandwidth applications. Intelligent technology selection-based on application requirements, channel conditions, and network state can optimize overall system performance [36].

Future optimization strategies may incorporate artificial intelligence, blockchain-based resource trading, and quantum enhanced security mechanisms. However, practical deployment will require careful consideration of computational requirements, energy constraints, and regulatory compliance across different jurisdictions.

2.6 Security and Privacy Framework

V2X security frameworks address unique challenges arising from highly dynamic network topologies, broadcast centric communication patterns and safety critical application requirements that demand both authentication and privacy preservation. This section examines the cryptographic mechanisms, certificate management systems and privacy preserving technologies that collectively enable secure V2X operations

2.6.1 IEEE 1609.2 Security Services

IEEE 1609.2 establishes comprehensive security services for WAVE-based V2X communications through PKI mechanisms optimized for vehicular environments [77]. The standard defines message authentication through the ECDSA with NIST P 256 curves [85], providing 128 bit security equivalent while maintaining computational efficiency suitable for real time safety applications.

Digital signature processing imposes significant computational overhead, with typical verification times ranging from 1-5 ms depending on hardware implementation. For applications requiring 10 Hz message transmission rates from multiple vehicles, signature verification becomes a performance bottleneck requiring hardware security modules or dedicated cryptographic accelerators. Advanced implementations employ signature verification queueing and prioritization to maintain real time processing capabilities [86]. Message encryption utilizes Elliptic Curve Integrated Encryption

Scheme (ECIES) to protect privacy sensitive unicast communications. The hybrid encryption approach employs ephemeral key agreement combined with symmetric encryption for computational efficiency. However, most V2X safety applications rely on broadcast communication where encryption is impractical, limiting the usage of ECIES to specific applications requiring confidentiality protection [87]. Certificate management in IEEE-1609.2 employs explicit certificate chains with butterfly key expansion mechanisms to enable efficient pseudonym generation. Long term enrollment certificates issued during vehicle manufacturing establish root trust relationships, while short term pseudonym certificates provide message signing capabilities with limited validity periods [88]. This approach balances authentication requirements with privacy protection by preventing long term vehicle tracking.

Critical analysis reveals potential vulnerabilities in the certificate provisioning and distribution mechanisms. The Security Credential Management System (SCMS) represents a complex infrastructure requiring coordination between multiple Certificate Authorities, creating potential single points of failure. Additionally, the explicit certificate approach incurs substantial message overhead (approximately 100+ bytes per signed message) that may affect bandwidth constrained applications.

2.6.2 ETSI Security Architecture and PKI

ETSI ITS security architecture, standardized through TS 103 097, TS 102 940, and TS 102 941, provides an alternative approach emphasizing implicit certificates and simplified trust management [88–90]. The architecture separates enrollment credentials for initial system access from authorization tickets enabling operational message signing, providing enhanced privacy protection through credential separation. Implicit certificate mechanisms reduce message overhead compared to explicit certificates by eliminating the need to transmit full certificate chains with each message. Certificate verification requires additional computational processing but results in smaller message sizes critical for bandwidth constrained safety applications. The trade off between computational overhead and message size optimization must be evaluated-based on specific deployment requirements.

Trust and Privacy Management (TPM) mechanisms implement sophisticated pseudonym management policies designed to balance authentication requirements with location privacy protection. Pseudonym change strategies consider vehicle mobility patterns, density conditions, and privacy threat models to optimize change timing and frequency. However, optimal pseudonym management requires accurate traffic density estimation and coordination between vehicles, presenting implementation challenges.

European PKI architecture emphasizes distributed trust management through multiple Certification Authorities (CAs) rather than centralized trust anchors. This approach provides enhanced resilience against CA compromise but complicates cross border interoperability and certificate validation procedures. Certificate Revocation Lists (CRLs) and Trust List management require efficient distribution mechanisms to maintain system security [91]. Misbehavior detection and reporting mechanisms enable the identification and exclusion of vehicles exhibiting malicious or erroneous behavior. Detection algorithms analyze message consistency, plausibility, and correlation with observed vehicle behavior to identify potential security threats [92]. However, the distributed nature of misbehavior detection creates challenges in achiev-

ing consensus and preventing false positive reports that could exclude legitimate vehicles.

2.6.3 Certificate Management and Pseudonym Systems

Large scale V2X deployments require sophisticated certificate management systems capable of supporting millions of vehicles with dynamic pseudonym provisioning and revocation capabilities. Certificate lifecycle management encompasses initial enrollment, periodic reauthorization, pseudonym issuance, and revocation processing. Each phase presents unique technical and operational challenges that affect the system's scalability and reliability. Initial vehicle enrollment typically occurs during manufacturing or first registration, establishing long term cryptographic identities and trust relationships. Enrollment procedures must verify vehicle authenticity, owner identity, and regulatory compliance while maintaining privacy protection. The enrollment process creates foundational trust relationships that allow subsequent authorization and pseudonym issuance [93].

Pseudonym provisioning systems must generate and distribute large numbers of short term certificates while maintaining unlinkability between pseudonyms and vehicle identities. Typical deployments require hundreds of pseudonym certificates per vehicle per year, creating substantial computational and storage requirements for PKI infrastructure. Efficient pseudonym generation algorithms and distribution mechanisms are critical for system scalability [94]. Certificate revocation presents particularly challenging requirements in V2X systems where revoked certificates must be rapidly distributed to prevent their continued use in safety critical applications. Traditional CRLs may be too large for efficient wireless distribution, requiring compressed revocation mechanisms or alternative approaches such as short lived certificates that expire rapidly [93, 95].

Privacy protection mechanisms must prevent correlation between different pseudonym certificates used by the same vehicle while enabling legitimate law enforcement and liability determination. Privacy preserving pseudonym management requires sophisticated cryptographic techniques and careful system design to prevent privacy breaches through traffic analysis or other correlation attacks [96].

2.6.4 Cross Technology Security Interoperability

Security interoperability between different V2X technology families represents a critical challenge for global deployment scenarios where vehicles must operate across regional boundaries with different security frameworks. While IEEE 1609.2 and ETSI TS 103 097 [88] maintain compatible cryptographic primitives, procedural differences in certificate management and trust establishment create interoperability barriers.

Cross border vehicle operation requires recognition of foreign security credentials and trust relationships. Mutual recognition agreements between regional PKI systems can enable limited interoperability, but require careful negotiation of security policies and operational procedures [97]. Technical gateway systems may provide certificate translation capabilities, but introduce additional complexity and potential security vulnerabilities [64]. C-V2X security integration with traditional V2X PKI systems [91] requires careful coordination of authentication mechanisms and security contexts. While PC5 interface security maintains compatibility with IEEE 1609.2 message

protection, integration with 5G authentication and key agreement procedures presents additional complexity. Network assisted security services through the Uu interface enable enhanced capabilities but create dependencies on cellular infrastructure availability [98, 99].

Future standardization efforts toward harmonized global V2X security frameworks may address some interoperability challenges. However, existing deployments, regulatory requirements, and national security considerations will likely maintain some degree of regional fragmentation. Practical V2X deployments must incorporate security gateway capabilities and multi stack certificate management to operate effectively across different regional security domains [100, 101].

The evolution toward quantum resistant cryptographic algorithms presents additional interoperability challenges as different regions may adopt different post quantum cryptographic standards at different timelines. V2X security architectures must incorporate crypto agility mechanisms that allow algorithm updates without requiring complete system replacement.

2.6.5 Integrity and Non-Repudiation in V2X PKI

The V2X security framework ensures message integrity and conditional accountability through architectural choices that balance security requirements with privacy mandates. Message integrity is inherently coupled with authentication, as IEEE 1609.2-2022 mandates that all BSMs and CAMs be signed using ECDSA over NIST P-256 curves [77]. Any alteration to a signed payload invalidates verification, making integrity an inseparable property of authenticated messages [96]. Rather than enforcing full non-repudiation, V2X systems adopt privacy preserving pseudonymous authentication, with frequent certificate rotation to prevent long-term vehicle tracking [88, 89]. Full non-repudiation would require persistent identity linkage, conflicting with GDPR compliant privacy by design principles [102]. Instead, conditional accountability is employed: message recipients verify legitimacy, while only authorized entities can resolve pseudonyms to long term identities under legally defined conditions such as misbehavior investigation or law enforcement requests, as specified by ETSI TS 102 941 and IEEE 1609.2.1 [90, 96].

2.6.6 Deployment Status and Interoperability

Real-world deployments empirically validate IEEE 1609.2 and ETSI TS 103 097 security architectures while exposing challenges in large-scale PKI operation and cross-border interoperability. In North America, USDOT Connected Vehicle Pilot programs and statewide deployments have demonstrated IEEE 1609.2-compliant SCMS operation at scale, supported by retained ITS spectrum [103–105]. In Europe, the C-ROADS platform enables harmonized Day 1 C-ITS services across multiple member states using ETSI ITS-G5 security, reinforced through interoperability Plugtests [106]. Asia-Pacific initiatives, including China's LTE-V2X mandates, South Korea dual-technology spectrum allocation, and Japan's long-standing V2I systems, further demonstrate operational maturity [107, 108]. Interoperability efforts led by OmniAir, IEEE 1609.2.1, and 5GAA address certification, trust federation, and DSRC-to-C-V2X transition challenges [106, 109]

2.6.7 V2X Service Classification and Requirements

V2X services span safety critical systems, cooperative driving, and non safety applications. Understanding service taxonomy and performance requirements is essential for cybersecurity risk assessment, as threat impact severity correlates with service criticality. Services are categorized by safety criticality, latency/reliability requirements, message types, and governing standards (SAE, ETSI, 3GPP).

Table 2.2: V2X Service Category Summary with Performance Requirements

Service Category	**Example Services**	**Latency Req.**	**Reliability**	**Primary Messages**
Safety-Critical (Active Safety)	Forward Collision Warning, Emergency Electronic Brake Light, Intersection Movement Assist	3-100ms	99-99.99%	BSM, CAM, DENM, SPaT
Cooperative Driving (Efficiency & Automation)	Cooperative Adaptive Cruise Control, Platooning, Cooperative Lane Change	50-200ms	99-99.9%	BSM, CAM, MCM
Traffic Efficiency (Non-Safety)	Traffic Information, GLOSA, Queue Warning, Parking Availability	500ms-1s	90-95%	SPaT, MAP, TIM, DENM
Infotainment & Convenience (Non-Safety)	Media Download, POI Notification, Remote Vehicle Control	1-5s	80-90%	Custom (IP-based)

Table 2.2 presents four V2X service categories. The service taxonomy establishes explicit quantitative links between service criticality and communication requirements, forming the basis for the cybersecurity risk assessment presented in Chapter 3. Safety critical services, characterized by ultra low latency (sub-100 ms) and extremely high reliability (99.999%), represent the highest risk category, as successful attacks can directly compromise occupant safety. Cooperative driving services exhibit moderate risk: while attacks may degrade system performance and efficiency, vehicles can typically rely on fallback mechanisms to maintain safe operation. Traffic efficiency and infotainment services pose lower immediate safety risks; however, they remain relevant from a security perspective, as they can serve as indirect attack vectors through privacy violations or denial-of-service propagation. Consequently, a risk based security strategy prioritizes strong authentication and anomaly detection for safety critical services. Chapter 3 formalizes this approach by introducing quantitative methodologies that jointly consider service criticality, threat likelihood, and potential attack impact.

2.7 Regulatory Framework and Spectrum Management

The regulatory landscape governing V2X communications involves spectrum allocation, emission standards, safety regulations, and cross border harmonization. Figure 2.11 illustrates regional spectrum designations, across major markets including Europe (5.875 5.905 GHz), US (5.895 5.925 GHz), and Asia Pacific. This section examines regional regulatory approaches, spectrum management strategies, and the evolving policy framework affecting V2X technology selection and deployment.

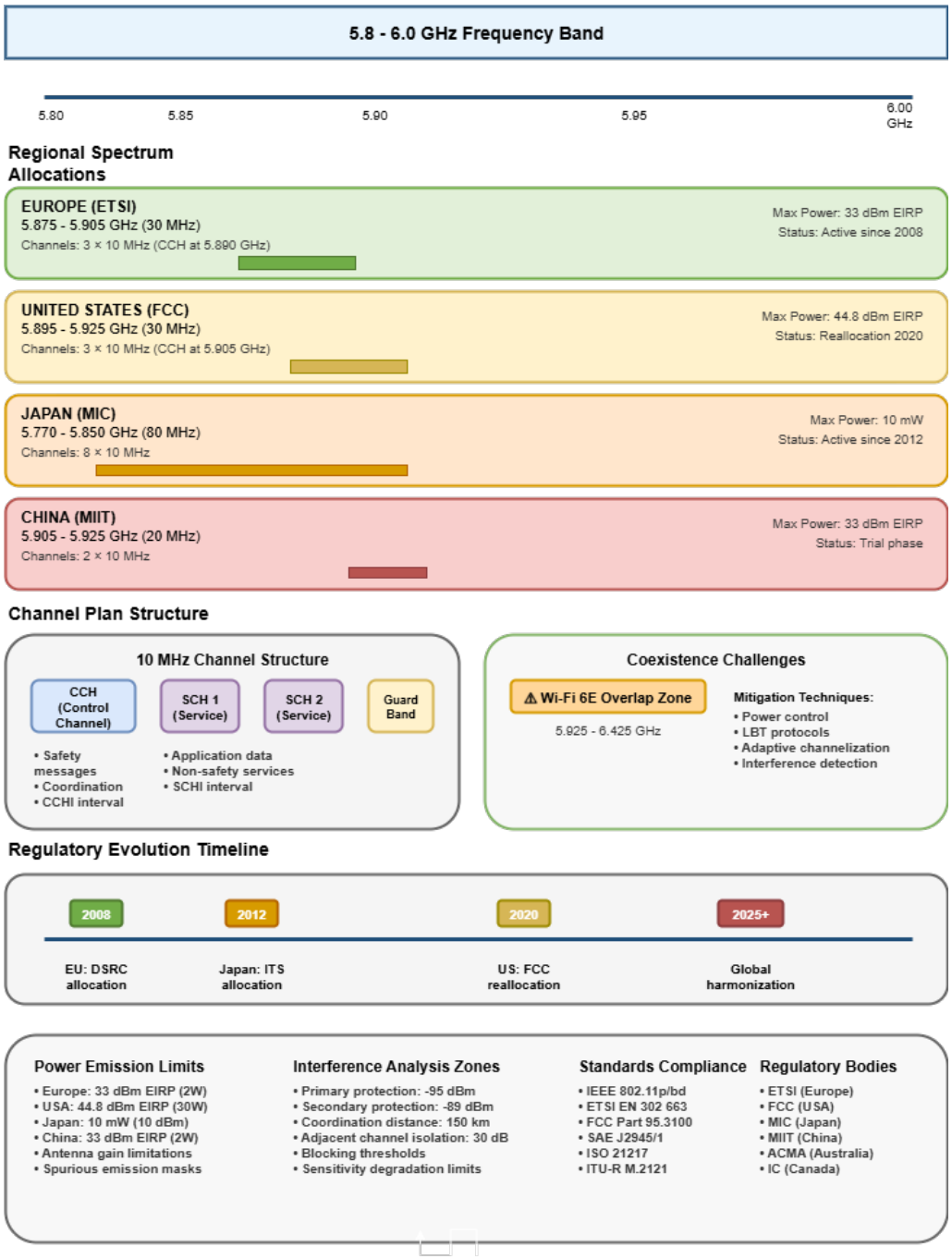


Figure 2.11: Global V2X Spectrum Allocations and Regulatory Framework.

2.7.1 Regional Spectrum Allocations

European V2X spectrum allocation follows ETSI harmonized standards that allocates 30 MHz within 5.875 5.905 GHz for ITS G5 operations, with technical parameters defined by EN 302 663 and radio conformance requirements specified in EN 302 571 [44, 80], as shown in Figure 2.11. The allocation provides seven 10 MHz channels enabling Control Channel/Service Channel separation or flexible single technology deployment strategies.

US spectrum policy, reallocated the 5.9 GHz band to address competing spectrum demands [105, 110]. These allocation designates 30 MHz (5.895 5.925 GHz) for transportation safety applications while reassigning the lower 45 MHz (5.850 5.895 GHz) primarily for unlicensed use including Wi-Fi 6E operations. This reallocation creates coexistence challenges between V2X and unlicensed operations. Asian markets exhibit diverse approaches reflecting different technological preferences and regulatory philosophies. Japan allocates 5.770 5.850 GHz for ITS applications with specific provisions for truck platooning and automated driving systems, as shown in Figure 2.11. South Korea emphasizes the deployment of C-V2X with spectrum allocations that supports both dedicated ITS bands and cellular spectrum sharing. China implements comprehensive C-V2X deployment policies with integrated spectrum and infrastructure development plans. Critical analysis reveals substantial challenges in achieving global spectrum harmonization. Existing spectrum allocations, incumbent services, and national policy priorities create barriers to unified global approaches. The impact extends beyond technical interoperability to affect equipment design, manufacturing costs, and deployment strategies for multinational automotive manufacturers.

2.7.2 Regulatory Compliance Requirements

Certification of V2X equipment requires compliance with multiple regulatory frameworks that encompasses radio emission standards, safety regulations, cybersecurity requirements, and privacy protection mandates. European compliance follows the Radio Equipment Directive (RED) 2014/53/EU with specific requirements detailed in ETSI EN 302 571 for 5.9 GHz ITS equipment [80]. Conformance testing addresses spectral mask requirements, out of band emissions, receiver performance standards, and electromagnetic compatibility.

United States certification follows FCC Part 95 rules with specific provisions for DSRC equipment and emerging C-V2X systems. The regulatory transition to C-V2X technologies requires updated certification procedures that addresses C-V2X technical characteristics while maintaining interoperability with legacy DSRC deployments during the transition period.

Cybersecurity regulations increasingly affect V2X deployments through requirements for security by design, vulnerability disclosure procedures, and incident reporting mechanisms. European cybersecurity regulations under the forthcoming Cyber Resilience Act [111] will impose specific requirements on connected vehicle systems, including V2X communications. Similar regulatory developments in other jurisdictions create compliance challenges for global automotive manufacturers.

Privacy protection regulations, including GDPR in Europe and various state privacy laws in the United States, impose requirements on V2X systems that collect, process, or transmit personal data. Although V2X safety applications typically

avoid personally identifiable information, location tracking capabilities and possible correlation with other data sources create privacy compliance obligations requiring careful system design and operational procedures [102].

Type approval procedures for V2X equipment vary significantly between regions, complicating global product development and deployment strategies. Mutual recognition agreements and harmonized certification procedures could reduce compliance costs and accelerate deployment, but require substantial coordination between regulatory authorities with different policy priorities and technical preferences.

2.7.3 Cross Border Interoperability Challenges

Cross border vehicle operation creates substantial regulatory and technical challenges that affect V2X system design and deployment strategies. Vehicles traveling between regions with different spectrum allocations, technical standards, and security frameworks must maintain operational capability while complying with local regulations. This requirement drives demand for multi technology, multi band V2X systems with associated cost and complexity implications [39, 40]. International coordination mechanisms through ITU R Working Party 5A address some harmonization challenges, but progress is limited by national sovereignty over spectrum allocation and telecommunications regulation. Regional standards bodies (ETSI, IEEE, 3GPP) maintain liaison relationships to promote interoperability, but fundamental differences in technical approaches and policy objectives create barriers to complete harmonization [63].

Automotive manufacturers face particular challenges in developing global vehicle platforms capable of operating across different regulatory environments. Multi band radio systems, region specific software configurations, and flexible security credential management systems are necessary but increase system complexity and cost. Over the air update capabilities may enable some regional adaptation, but hardware constraints and certification requirements limit flexibility. Cross border security credential recognition presents additional operational challenges requiring mutual trust relationships between different PKI systems and security frameworks [91]. While technical interoperability between IEEE 1609.2 [10] and ETSI TS 103 097 [88] security frameworks is possible, operational procedures and trust policies. differ substantially between implementations.

Future regulatory development toward increased harmonization faces political and economic constraints that limit progress toward unified global approaches. Trade policy considerations, technology sovereignty concerns, and domestic industry protection may prevent comprehensive international cooperation despite the technical benefits of harmonized V2X systems.

2.8 Implementation Challenges and Research Directions

Contemporary V2X deployment faces multifaceted challenges spanning technical limitations, economic constraints, and systemic integration requirements that collectively influence technology adoption trajectories and research priorities. This section examines critical implementation barriers and identifies promising research directions

for next generation V2X systems.

2.8.1 Scalability and Performance Limitations

Scalability analysis reveals fundamental performance limitations as V2X networks approach high vehicle densities projected for mature autonomous vehicle deployments. IEEE-802.11p CSMA/CA medium access exhibits exponential performance degradation with Packet Delivery Ratio falling below acceptable thresholds (>95%) when CBR exceeds 0.7 in typical urban scenarios [41]. Mathematical modeling demonstrates that current DCC mechanisms provide insufficient performance improvement for extreme density scenarios where hundreds of vehicles may operate within single communication ranges. The reactive nature of CBR-based congestion control creates stability challenges and potential oscillatory behavior under rapidly changing traffic conditions.

C-V2X technologies provide improved scalability characteristics through scheduled resource allocation, but face limitations in resource pool efficiency and sensing accuracy for Mode 4 autonomous operation. As vehicle density increases, resource collision probability grows despite sensing-based selection algorithms, requiring more sophisticated resource allocation and interference mitigation techniques [33, 112].

Network infrastructure scalability presents additional challenges for hybrid V2X deployments combining direct communication with network assisted services. RSU deployment density requirements scale non linearly with traffic density and application performance requirements [113]. Edge computing resource allocation and management across distributed RSU infrastructure requires sophisticated orchestration mechanisms that remain largely unproven at scale [114]. Research directions include ML enhanced resource allocation algorithms, cooperative sensing mechanisms to improve resource selection accuracy, and hierarchical network architectures that can adapt resource allocation strategies-based on local density conditions and application requirements [115, 116].

2.8.2 Security Implementation at Scale

Large scale V2X security implementation presents operational challenges that extend beyond cryptographic algorithm performance to encompass certificate lifecycle management, misbehavior detection, and privacy preservation under realistic attack scenarios. PKI scalability analysis indicates that supporting millions of vehicles with dynamic pseudonym provisioning requires infrastructure capabilities significantly exceeding current implementations [91]. Certificate distribution and revocation mechanisms face particular scalability challenges where rapid revocation of compromised credentials is essential for safety critical applications. Traditional CRL-based approaches may be inadequate for large scale deployments due to bandwidth requirements and update latency constraints [94]. Short lived certificates and innovative revocation mechanisms including probabilistic data structures show promise but require substantial additional research.

Misbehavior detection systems must operate in highly dynamic environments where normal vehicle behavior exhibits substantial variation due to traffic conditions, weather, driver behavior, and vehicle capabilities [92]. False positive rates in misbehavior detection can lead to inappropriate vehicle exclusion, while false negatives

may allow malicious vehicles to continue operating. Achieving optimal detection performance requires sophisticated algorithms that incorporate multiple data sources and behavioral modeling techniques. Privacy preservation under advanced attack scenarios including long term observation, traffic analysis, and correlation with other data sources requires more sophisticated privacy protection mechanisms than current pseudonym-based approaches provide. Differential privacy techniques, homomorphic encryption, and zero knowledge proof mechanisms may enable enhanced privacy protection, but require substantial computational resources and protocol modifications [53]. Research priorities include distributed misbehavior detection algorithms, privacy preserving authentication mechanisms, quantum resistant cryptographic implementations, and adaptation of autonomous security parameters based on threat intelligence and observed attack patterns [117].

2.8.3 Cross Technology Coexistence

The coexistence of multiple V2X technologies within shared spectrum allocations creates complex interference management and resource coordination challenges that current standards address inadequately. IEEE-802.11p and LTE-V2X systems operating in the same 5.9 GHz band require sophisticated coexistence mechanisms to prevent mutual interference while enabling technology migration strategies.

Listen Before Talk (LBT) mechanisms for LTE-V2X Mode 4 operation provide basic interference avoidance but may be insufficient for fair spectrum sharing with IEEE-802.11p systems that employ different medium access mechanisms [50, 118]. Power control coordination, spatial separation techniques, and temporal coordination mechanisms may be necessary to enable acceptable coexistence performance.

The introduction of Wi-Fi 6E operations in adjacent spectrum (United States) or potentially overlapping spectrum (other regions) creates additional coexistence challenges that may affect V2X system performance. Interference mitigation techniques, dynamic frequency selection, and transmit power adaptation mechanisms require careful optimization to maintain V2X application performance while enabling unlicensed spectrum usage. Technology transition strategies must consider legacy system compatibility, infrastructure migration costs, and user experience continuity during transition periods that may extend over decades. Hybrid OBU implementations supporting multiple V2X technologies provide flexibility but increase cost and complexity significantly. Software defined radio approaches may enable some adaptation but face limitations in real time processing requirements and power consumption constraints.

Research directions include intelligent spectrum sharing algorithms, ML enhanced interference prediction and mitigation, and protocol design techniques that enable graceful performance degradation under interference conditions while maintaining safety critical application functionality [119].

2.8.4 Future Research Opportunities

Emerging technologies including artificial intelligence, edge computing, blockchain, and quantum communications present substantial opportunities for next generation V2X systems that address current limitations while enabling novel applications and capabilities. ML techniques show promise for predictive resource allocation,

adaptive security parameter configuration, and intelligent protocol optimization-based on observed network conditions and application requirements. Federated learning approaches may enable cooperative algorithm training across vehicle fleets while preserving privacy through distributed learning mechanisms. This could enable adaptive misbehavior detection, personalized driver assistance applications, and cooperative perception algorithms that improve with experience while maintaining user privacy protection.

Blockchain and distributed ledger technologies offer potential solutions for decentralized security credential management, reputation systems for misbehavior detection, and resource trading mechanisms that could improve spectrum efficiency through market-based allocation strategies. However, the computational and energy requirements of blockchain systems require careful evaluation for vehicular applications with strict latency and power constraints. Quantum communication technologies may eventually provide fundamental security enhancements through quantum key distribution and quantum resistant authentication mechanisms. However, practical quantum communication systems remain decades away from vehicular deployment, requiring continued development of post quantum cryptographic approaches as an interim solution. 6G wireless technologies promise ultra low latency, massive connectivity, and integrated sensing capabilities that could transform V2X applications through cooperative perception, predictive safety systems, and seamless integration with smart city infrastructure. However, 6G standardization and deployment timelines suggest limited impact on near term V2X deployments [112, 120, 121].

Integrated sensing and communication approaches that combine sensing with communication functions could provide enhanced situational awareness while improving spectrum efficiency. These techniques require substantial advances in signal processing algorithms and antenna technologies but offer promising applications for cooperative perception and infrastructure free positioning systems.

2.9 Chapter Summary and Integration

This comprehensive analysis of V2X communication systems reveals a complex technological landscape characterized by competing standards, evolving regulatory frameworks, and substantial implementation challenges that collectively shape the trajectory toward large scale CITS. The critical evaluation presented demonstrates that no single V2X technology provides optimal performance across all application scenarios, necessitating hybrid deployment strategies that leverage complementary technology strengths.

- Technical Architecture Assessment: IEEE-802.11p [122]-based systems excel in ultra low latency applications requiring deterministic medium access, achieving $<$10 ms communication latencies essential for collision avoidance applications. However, scalability limitations become pronounced at vehicle densities exceeding 50-100 vehicles per communication range. C-V2X [123] technologies provide superior scalability and extended coverage through scheduled resource allocation but introduce additional complexity and infrastructure dependencies that may compromise reliability in coverage limited scenarios.

- Protocol Stack Interoperability: The analysis reveals fundamental architectural differences between WAVE [67], ITS G5 [65], and 3GPP C-V2X protocol

stacks [50, 124] that create substantial barriers to seamless interoperability. While security frameworks maintain compatible cryptographic mechanisms, message semantics, certificate management procedures, and network architecture approaches differ sufficiently to require gateway systems or multi stack implementations for cross technology operation.

- Regulatory and Spectrum Challenges: Regional spectrum allocation differences and evolving regulatory policies create ongoing uncertainty for global V2X deployment strategies. The United States' 5.9 GHz band reallocation and introduction of unlicensed coexistence requirements exemplify the dynamic regulatory environment affecting technology selection and deployment economics. Cross border interoperability requirements demand sophisticated multi band, multi standard vehicle implementations with associated cost implications.

- Security Framework Maturity: Current V2X security frameworks provide adequate cryptographic protection for message authentication and basic privacy preservation, but face scalability challenges when extended to support millions of vehicles with dynamic certificate management requirements. Misbehavior detection mechanisms remain largely theoretical, requiring substantial additional development for practical implementation. Privacy preservation under advanced attack scenarios including long term observation and traffic analysis requires enhanced protection mechanisms beyond current pseudonym-based approaches.

- Implementation Readiness Assessment: The technical analysis indicates that while individual V2X technologies have reached sufficient maturity for limited deployment scenarios, system level integration challenges remain substantial barriers to large scale implementation. Cross technology coexistence mechanisms, scalable security infrastructure, and hybrid protocol stack implementations require additional development before supporting the vehicle densities and application complexity anticipated for mature autonomous vehicle deployments.

- Research Direction Synthesis: Future research priorities must address scalability limitations through advanced resource allocation algorithms, enhanced security frameworks capable of supporting large scale deployments with sophisticated threat mitigation capabilities, and cross technology interoperability mechanisms enabling graceful migration between competing standards. ML enhanced optimization techniques, quantum resistant security implementations, and integrated sensing and communication approaches represent promising directions for next generation V2X systems.

The foundational understanding established in this chapter provides the technical context for the cybersecurity risk assessment methodologies examined in subsequent chapters. The identification of fundamental protocol limitations, interoperability challenges, and scalability constraints directly informs the threat modeling approaches and vulnerability assessment techniques that constitute the primary research contribution of this investigation. The technical vulnerabilities identified through this comprehensive protocol analysis including congestion control limitations, cross stack interoperability gaps, and scalable security implementation challenges establish the attack surface that will be systematically evaluated through the Software Defined

Radio-based vulnerability assessment framework developed in the following chapters. This foundational technical analysis thus provides both the contextual understanding and the specific target identification necessary for rigorous cybersecurity risk assessment in contemporary V2X systems.

Chapter 3

V2X cybersecurity Risk Management

3.1 Introduction

As outlined in Chapter 2, the rapid evolution of V2X communication, together with the adoption of advanced wireless standards, such as DSRC, LTE-V2X, and emerging 5G-V2X technologies, has introduced new layers of complexity and inter connectivity within ITS. While these technologies significantly improve road safety, traffic efficiency, and user experience, they also expand the attack surface of vehicular ecosystems, making them increasingly vulnerable to cyber threats. To address these challenges, several standards and guidelines have emerged, aimed at defining cybersecurity requirements for vehicular networks, with a central focus on the development of risk management methodologies capable of assessing, mitigating, and managing risks specific to V2X environments [117, 125].

V2X systems face cybersecurity challenges that differ markedly from those of conventional IT infrastructures. Unlike enterprise IT systems [126], which typically prioritize the confidentiality of data, V2X environments place greater emphasis on availability, reliability, integrity, and low latency performance. A disruption in vehicular communications, such as the loss of BSMs or interference with DSRC signal exchanges, may result not only in degraded performance but also in immediate safety hazards for drivers, passengers, and pedestrians. This fundamental difference highlights the need for a specialized approach to cybersecurity risk management tailored to the operational and safety critical characteristics of V2X communications [127].

Accordingly, this chapter explores practical strategies and frameworks for implementing cybersecurity risk management in V2X ecosystems, with a particular emphasis on DSRC-based communications and cellular V2X technologies. It begins with a discussion of core risk management concepts, adapted from standards such as ISO/SAE 21434/SAE J2735 (road vehicle cybersecurity engineering) [19, 46, 128], UNECE WP.29 Regulations R155/R156 [20], and NIST's cybersecurity frameworks [17, 129–131], and tailored to the vehicular domain. These frameworks are adapted and contextualized to address the unique requirements of the vehicular domain. Subsequently, the chapter examines approaches for defining the context and scope of cybersecurity risk management processes in V2X environments, considering both internal system vulnerabilities (e.g., DSRC protocol limitations, message authentication weaknesses) and external threats (e.g., jamming, spoofing, and MitM attacks).

Subsequent sections address the processes of risk assessment, focusing on the

identification and evaluation of threats and vulnerabilities specific to vehicular communication. The discussion then moves to risk treatment and mitigation strategies, including intrusion detection, cryptographic protection of safety messages, and redundancy in communication channels. Finally, the chapter highlights the importance of continuous monitoring and review, as V2X networks operate in highly dynamic contexts where both system configurations and threat landscapes evolve rapidly.

The chapter is structured as follows: Section 3.2 introduces the fundamental concepts of cybersecurity risk management for V2X, defining risk and outlining its key components. It also provides a comparative analysis of established standards such as ISO/SAE 21434, ETSI EN 302 665, UNECE WP.29 R155/R156, and the NIST framework in the context of vehicular networks.

Section 3.3 examines how organizations and stakeholders (e.g., vehicle manufacturers, infrastructure operators) can define the context and scope of risk management, with attention to both technical and operational risk factors.

Section 3.4 describes the process of conducting risk assessments for V2X systems, focusing on the identification of DSRC specific vulnerabilities, potential attack vectors, and their implications for safety critical applications.

Section 3.5 discusses strategies for treating and mitigating these risks, including cryptographic schemes, secure message dissemination protocols, and the integration of anomaly detection mechanisms.

Section 3.6 emphasizes the necessity of continuous monitoring and periodic reviews to ensure that V2X risk management practices remain adaptive to evolving cyber threats, vehicular technologies, and regulatory requirements.

3.2 Fundamental Concepts of V2X cybersecurity Risk Management

The paradigm of cybersecurity risk management within V2X ecosystems represents a fundamental departure from traditional information technology security frameworks. This departure emerges from the intrinsic safety critical nature of vehicular communication, where the consequences of security failures extend beyond data compromise to encompass immediate threats to human life and transportation system integrity [127]. The analytical framework developed herein addresses this paradigmatic shift by establishing risk management principles that inherently recognize the interdependence between cybersecurity and functional safety within highly dynamic vehicular environments. Figure 3.1 illustrates comprehensive V2X Risk Management Framework integrating asset identification, threat assessment, and mitigation strategies across vehicular communication infrastructure.

The foundational premise underlying V2X cybersecurity risk management posits that traditional security paradigms, which typically emphasize confidentiality as the paramount objective, prove inadequate when applied to safety critical vehicular communications. The empirical evidence supporting this assertion lies in the temporal constraints governing V2X operations, where BSMs [132] must be processed and acted upon within millisecond timeframes to maintain collision avoidance effectiveness [133]. This temporal criticality fundamentally alters the risk calculus, requiring security measures that preserve both information integrity and operational responsiveness under adversarial conditions.

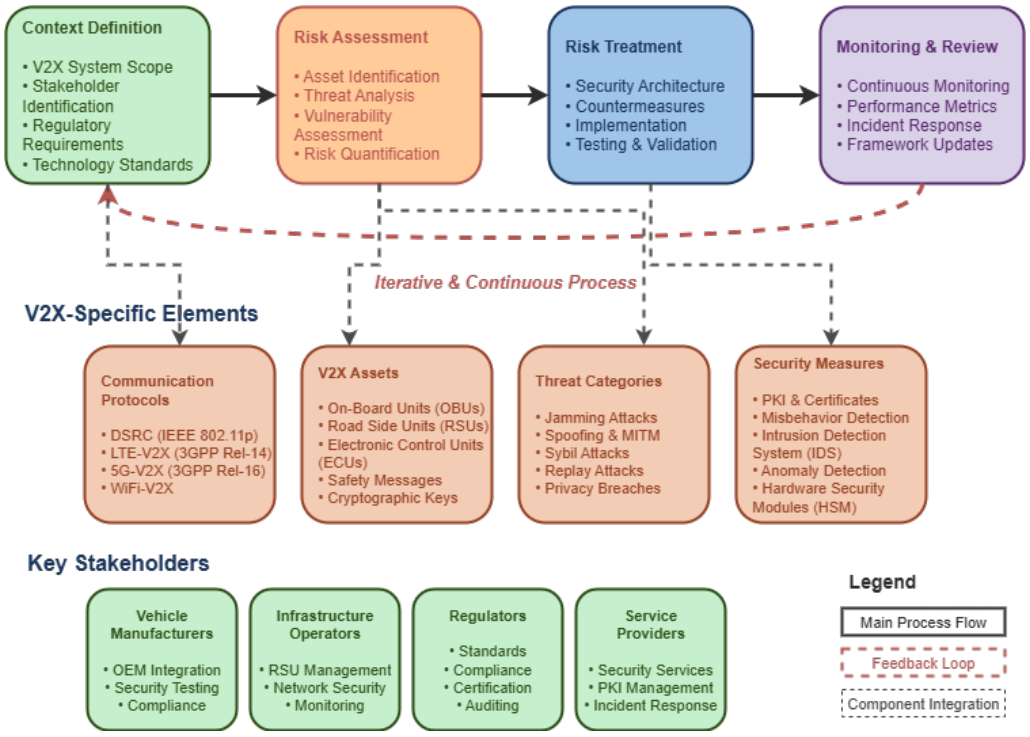


Figure 3.1: V2X Risk Management Framework

At its core, risk management in V2X is guided by the following key components:

- Risk Definition: Risk is generally understood as the likelihood that a threat will exploit a vulnerability, resulting in adverse consequences [134]. In the V2X context, this may involve an adversary exploiting protocol level weaknesses (e.g., DSRC message spoofing or jamming) that impact message integrity, authenticity, or timely delivery [135].

- Assets: The primary assets in V2X systems include not only hardware components (OBUs, RSUs, sensors, and ECUs) but also communication links and safety critical messages such as BSMs, CAMs, and DENMs [136]. Protecting the accuracy and availability of these assets is essential to maintaining road safety [137].

- Threats: Threats in V2X encompass a wide spectrum, including DoS and jamming attacks [133], message spoofing, Sybil attacks, and MitM exploits. These threats are often more severe than in enterprise IT systems because of their direct implications for physical safety.

- Vulnerabilities: Vulnerabilities arise from weaknesses in protocol design (e.g., lack of encryption in DSRC), implementation flaws, misconfigured systems, or insufficient authentication mechanisms. The inherent mobility and dynamic topological characteristics of vehicular networks compound these vulnerabilities by creating temporal windows of opportunity that adversaries can exploit[127].

- Impact: The impact of a successful cyberattack on V2X systems extends beyond data compromise to physical harm, traffic disruptions, loss of human lives, economic losses, and erosion of public trust in ITS.

- Controls and Countermeasures: Effective risk management incorporates both preventive and corrective measures, including cryptographic authentication of safety messages, secure key distribution schemes, IDS, redundancy across communication channels (DSRC + LTE-V2X/5G), and anomaly detection based on vehicular context.

Several international frameworks establish the foundation for structuring cybersecurity risk management within V2X ecosystems. As illustrated in Figure 3.2, the V2X Asset Classification and Threat Landscape analysis identifies critical system components and their corresponding cybersecurity vulnerabilities, serving as a basis for systematic risk assessment. The ISO/SAE 21434 standard [138] specifically addresses cybersecurity for road vehicles by introducing a lifecycle-oriented approach to risk management that spans the entire vehicle development process—from concept and design to production, operation, and eventual decommissioning. Complementing this, the UNECE WP.29 Regulations R155 and R156 [139, 140] mandate the implementation of CyberSecurity Management Systems (CSMS) and Software Update Management Systems (SUMS) for automotive manufacturers. These regulations emphasize continuous risk assessment, threat monitoring, and incident response to ensure sustained protection throughout a vehicle's operational life. In parallel, ETSI EN 302 665 [141] defines the communication architecture and security requirements for C-ITS, providing guidelines for secure message exchange and interoperability among V2X entities. Collectively, these frameworks establish a comprehensive basis for managing cybersecurity risks in connected vehicular environments.

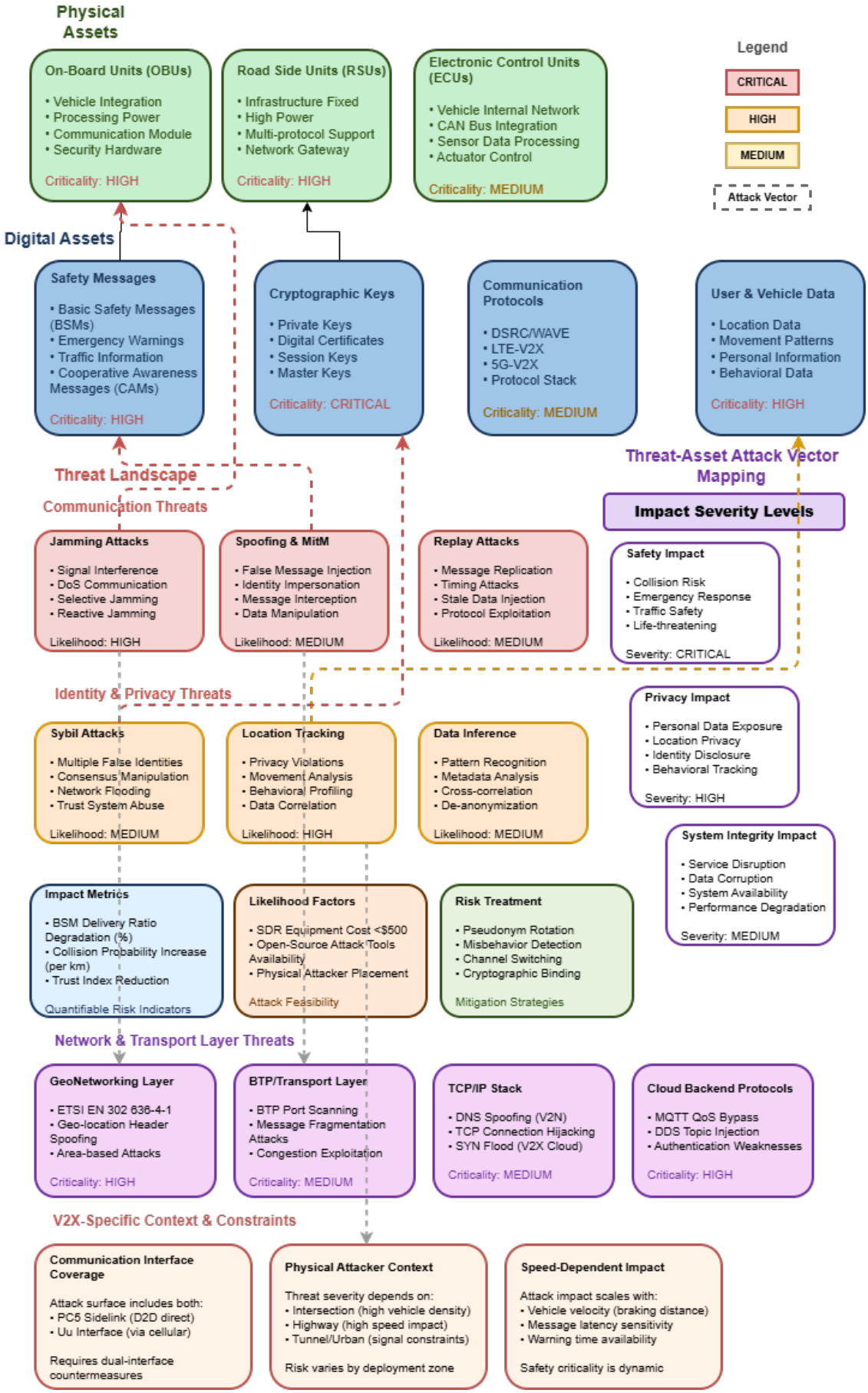


Figure 3.2: V2X Asset Classification and Threat Landscape Analysis

3.2.1 Regional Security Framework Differences

Regional variations in security architectures for V2X communications reflect differing regulatory priorities and approaches to balancing privacy, trust, and accountability. In Europe, ETSI TS 102 940 [89] defines the trust and privacy management framework for Cooperative C-ITS, introducing pseudonymous authentication as the primary mechanism to preserve user privacy. This approach ensures that vehicle identities remain unlinkable across communication sessions, thereby safeguarding location privacy. Complementing this, ETSI TS 103 097 [142] specifies the security header formats and message structures used for signed V2X communications, optimizing both message verification efficiency and bandwidth utilization, which are critical for latency-sensitive safety applications.

In contrast, the North American Security Credential Management System (SCMS) adopts a different trust philosophy. It emphasizes certificate transparency and controlled linkability to support misbehavior detection and forensic analysis [92]. While this model enhances the system's ability to identify and isolate malicious entities, it does so by introducing limited linkability among certificates potentially increasing privacy risks compared to the European model. Consequently, these architectural and policy-level differences influence cybersecurity risk assessment methodologies: privacy centric frameworks may offer stronger data protection but reduced visibility into attack patterns, whereas linkability based systems enable more effective monitoring at the expense of some user privacy.

Beyond regional frameworks, general cybersecurity standards, such as NIST SP 800-30 and the NIST Cybersecurity Framework (CSF) [143, 144], provide foundational principles for risk identification, assessment, and mitigation. However, these frameworks require contextual adaptation to address the dynamic, real time, and safety critical nature of vehicular networks. Similarly, the ISA/IEC 62443 series [145], originally designed for industrial control systems, offers transferable methodologies for assessing vulnerabilities and securing distributed, safety-relevant systems like V2X infrastructures.

In summary, the cybersecurity risk management of V2X ecosystems extends beyond conventional IT paradigms by integrating operational, safety, and performance considerations inherent to vehicular environments. By clearly defining assets, threats, vulnerabilities, and impacts within this specialized context, organizations can develop risk management strategies that are both technically robust and safety-oriented, forming the foundation for subsequent processes of context definition, risk assessment, and mitigation.

3.2.2 V2X-Specific Security Characteristics

While V2X communications share some vulnerabilities with generic wireless networks (jamming, eavesdropping, replay attacks), the vehicular context introduces six quantitative differentiators that fundamentally distinguish V2X cybersecurity from other domains such as telemedicine, industrial IoT, or aviation communications. These characteristics create unique security engineering challenges that require domain specific solutions.

Millisecond Latency Constraint

V2X safety applications impose exceptionally strict real-time constraints on security operations. SAE J2945/1 mandates that Basic Safety Messages (BSMs) be processed within 100 ms from transmission to application-level decision-making, with collision avoidance functions often requiring reactions within 50 ms of threat detection [146, 147]. As a result, cryptographic signature verification, certificate validation, and misbehavior detection must execute within this sub-100 ms window on resource-constrained vehicular platforms. These requirements are one to two orders of magnitude more stringent than other safety-critical wireless systems, such as telemedicine (150–300 ms latency) [148], industrial IoT supervisory control (1–10 s control loops), and aviation ADS-B position reporting (1 s update intervals) [149]. Consequently, the V2X security stack must rely on highly optimized cryptographic primitives and scalable revocation mechanisms to meet latency constraints without compromising safety application responsiveness

Broadcast Centric Communication with Privacy Requirements

V2X security operates in a fundamentally broadcast dominated paradigm with stringent privacy constraints. Unlike cellular networks where authentication occurs once during connection establishment, each V2X vehicle broadcasts BSMs at 10 Hz (SAE J2735) [146, 147], and each message requires individual cryptographic authentication. At a moderately congested intersection with 50 vehicles, a receiving vehicle must authenticate 500 messages per second each containing an ECDSA-256 signature and a pseudonym certificate.

This broadcast model creates three simultaneous security requirements absent in other wireless domains: (1) per message authentication to prevent injection of false kinematic data, (2) sender pseudonymity to prevent long-term vehicle tracking, and (3) misbehavior detection to identify compromised credentials without centralized revocation synchronization. The combination of high message rates, per-message cryptographic overhead, and privacy preserving certificate management (vehicles rotate pseudonym certificates every 5-20 minutes per IEEE 1609.2) [10] creates a computational and storage burden unique to V2X. Industrial IoT networks may use group authentication or session based security, and aviation systems broadcast unauthenticated ADS-B messages, making neither approach applicable to V2X's trust model.

Physical Kinetic Consequences with Sub-Second Time-to-Impact

The coupling between cyber attacks and vehicle kinematics creates sub second consequence timescales unmatched in other wireless domains. At highway speeds of 130 km/h (36 m/s), a 1-second communication loss corresponds to 36 meters of unprotected travel, preventing collision detection in crossing path scenarios [146, 147]. Injection of false BSMs, such as emergency brake events, can trigger automated emergency braking in following vehicles, potentially causing collisions within 2–3 seconds. These time to consequence constraints far exceed those in telemedicine, where clinical review introduces seconds to minutes latency [148], and industrial SCADA systems, which rely on process inertia with seconds to hours response. Even aviation systems operate with larger separation buffers (5–10 nautical miles)

and human intervention, despite higher speeds [149]. Consequently, V2X security mechanisms including intrusion detection and message plausibility validation must function on sub-second timescales to prevent direct kinetic impacts.

Heterogeneous Protocol Stack with Multiple Attack Surfaces

V2X-enabled vehicles must simultaneously secure an unprecedented combination of communication technologies within a single platform. A production V2X system integrates: DSRC (IEEE 802.11p) operating in the 5.9 GHz ITS band, C-V2X (3GPP Release 14/15) on licensed cellular spectrum, GNSS positioning (GPS, GLONASS, Galileo) for localization, in-vehicle CAN/CAN-FD networks for actuator control, and automotive Ethernet for high-bandwidth sensor fusion. Each protocol presents distinct attack surfaces—802.11p frame injection, LTE-V sidelink resource allocation attacks, GNSS spoofing, CAN message injection—that must be defended holistically.

This heterogeneity is unique to V2X. Telemedicine systems predominantly use TLS-secured IP over cellular or WiFi. Industrial IoT deployments may mix protocols (Modbus, OPC-UA) but within segmented network zones. Aviation uses dedicated VHF datalinks (VDL Mode 2, CPDLC) with separation from passenger WiFi. The V2X security architecture must provide cross-layer defense (e.g., correlating GNSS-derived position in BSMs with DSRC-received kinematics to detect spoofing) while maintaining real-time performance across all interfaces.

Dynamic Network Topology with Infrastructure-Independent Trust

V2X networks exhibit extreme topological dynamics that preclude traditional infrastructure-dependent security models. At relative speeds up to 500 km/h (opposing highway traffic at 250 km/h each), neighbor vehicle sets change completely within seconds. A vehicle entering a tunnel or rural area may lose cellular backhaul connectivity for minutes while still requiring V2X security services. Trust establishment, misbehavior detection, and credential revocation must therefore function in intermittently connected, infrastructure independent modes.

This contrasts sharply with cellular IoT (persistent base station connectivity), WiFi networks (fixed access point topology), and even mobile ad-hoc networks in military contexts (where units move in coordinated formations). V2X security protocols must support decentralized trust models such as collective detection of misbehavior through multi-vehicle consensus mechanisms and forward-secure cryptographic credentials that remain valid during temporary disconnection. The ETSI ITS-G5 DENM system, for example, enables peer-to-peer hazard alert propagation without infrastructure coordination, requiring security mechanisms that validate message authenticity through distributed plausibility checks rather than centralized validation.

Regulatory Safety Mandate with Type Approval Implications

Unlike most wireless communication systems where cybersecurity is a voluntary best practice, V2X security is subject to international vehicle type-approval regulations. UN Regulation 155 (Cyber Security Management System) and UN Regulation 156 (Software Update Management System) [139], entering force in July 2024 for new vehicle types, mandate cybersecurity as a prerequisite for vehicle homologation.

ISO/SAE 21434 (Road Vehicles—Cybersecurity Engineering) [19] establishes engineering processes for threat analysis and risk assessment throughout the vehicle lifecycle, with specific clauses addressing V2X communication security.

This regulatory framework creates enforceable consequences absent in other domains: a demonstrated cybersecurity vulnerability in a V2X system can result in type approval suspension, effectively prohibiting vehicle sales. In contrast, telemedicine device security follows FDA guidance (premarket cybersecurity for medical devices) but lacks hard certification gates, and industrial IoT security remains largely governed by voluntary standards (IEC 62443). Aviation cybersecurity is regulated (DO-326A/ED-202A), but applies primarily to avionics software rather than communication protocols. The V2X regulatory mandate thus elevates security from a design consideration to a legal requirement, necessitating rigorous documentation, testing, and certification processes specific to vehicular threat models.

3.2.3 Cause-Effect-Consequence Framework

The six characteristics above demonstrate a hierarchical causal chain linking technical constraints to physical outcomes:

- **Root Cause**: V2X operational requirements (low latency, broadcast architecture, real-time control coupling).
- **Intermediate Effect**: Security mechanisms must operate under unprecedented combined constraints: sub-100ms processing windows, 500 msg/sec authentication rates, dynamic topology, multi-protocol integration, and regulatory mandates.
- **Consequence**: Security mechanisms designed for domains such as enterprise IT, industrial IoT, or aviation are not directly transferable to V2X environments. In traditional systems, trade-offs between security strength and latency can often be balanced through buffering, centralized processing, or delayed decision-making. In contrast, V2X applications operate under strict real-time and safety-critical constraints, where even millisecond-level delays may directly affect vehicle kinematics and collision avoidance outcomes. As a result, conventional security performance trade-off strategies become inadequate. V2X systems require domain specific security architectures that integrate ultra-low-latency cryptographic validation, distributed trust management, real-time anomaly detection, and resilience to wireless interference, all while preserving privacy. These challenges and their quantitative implications are further formalized in Section 3.4.3, where risk parameters are derived based on service criticality, temporal constraints, and attack impact.

Table 3.1 presents a quantitative comparison of latency budgets across safety-critical wireless domains. This comparison reveals that V2X operates under fundamentally different temporal constraints than comparable systems, requiring security mechanisms designed from first principles rather than adapted from other domains.

The data demonstrates that V2X safety applications occupy a unique niche: tighter latency constraints than telemedicine and aviation, but without the process inertia buffer available to industrial SCADA systems. This combination necessitates

Table 3.1: Cross-Domain Latency Comparison for Safety-Critical Wireless Systems

Domain	**Latency Budget**	**Security Window**	**Consequence of Failure**
V2X Safety (DSRC)	100 ms	10-20 ms	Collision warning reaches vehicle too late; emergency braking disabled
Telemedicine	200-500 ms	50-100 ms	Delayed diagnosis; clinical review buffers errors
Industrial IoT (SCADA)	10-100 ms	5-10 ms	Equipment damage; process inertia provides recovery window
Aviation ADS-B	1000 ms	100-200 ms	Reduced separation between aircraft; ATC coordination delays

security mechanisms that operate at sub-20ms decision latency while maintaining cryptographic and authentication rigor a requirement unmatched in other wireless domains.

3.3 Context and Scope Definition for V2X Risk Management

Defining the context and scope of cybersecurity risk management is a critical step in ensuring that the process addresses the unique characteristics of V2X communication systems. Unlike enterprise IT networks, which often have relatively stable infrastructures, V2X environments are highly dynamic, heterogeneous, and safety critical. As such, risk management strategies must consider not only the technical dimensions of communication protocols but also the operational, regulatory, and societal contexts in which these systems function.

The internal context of V2X risk management includes the technical infrastructure and resources that directly contribute to vehicular communication. This encompasses OBUs, RSUs, ECUs, and the communication protocols such as DSRC, LTE-V2X, and 5G-V2X that facilitate message exchange. It also includes the operational requirements of V2X systems, where ultra-low latency, message reliability, and continuous availability are paramount for road safety applications. For example, the integrity and timelines of CAMs and BSMs are vital to preventing collisions and ensuring cooperative driving as explained in section 3.2. Internally, the scope must also account for existing controls, such as cryptographic authentication mechanisms, IDS, and anomaly detection algorithms embedded within vehicular platforms.

3.3.1 Compliance with Security Standards

The harmonization of V2X cybersecurity implementations with established international standards represents a critical success factor in achieving interoperability,

regulatory compliance, and the establishment of a consistent industry-wide security baseline. This section examines the integration of V2X specific risk management frameworks with broader automotive cybersecurity standards, emphasizing both the shared foundational principles and the domain specific adaptations required for effective vehicular security governance.

The primary standards governing V2X cybersecurity include ISO/SAE 21434 [138], which defines lifecycle based risk management practices for automotive cybersecurity engineering; UNECE WP.29 Regulations R155 and R156 [20], which specify requirements for cybersecurity and SUMS; ETSI EN 302 665 [2], which outlines the ITS communication architecture and associated security mechanisms; and IEEE 1609.2 [77], which defines the security architecture for WAVE. These standards, established by recognized bodies, such as ETSI, IEEE, and the Society of Automotive Engineers (SAE), collectively define the mandatory security, communication, and compliance frameworks that underpin C-ITS. Figure 3.3 presents a Security Standards Compliance Matrix, illustrating the interrelationship between key international standards—ISO/SAE 21434, UNECE R155/R156, ETSI EN 302 665, and IEEE 1609.2 and their respective coverage of critical cybersecurity requirements. The matrix categorizes requirements such as risk management, incident response, continuous monitoring, security updates, authentication, privacy protection, and vulnerability management, indicating whether each is mandatory, partially covered, or limited across the standards.

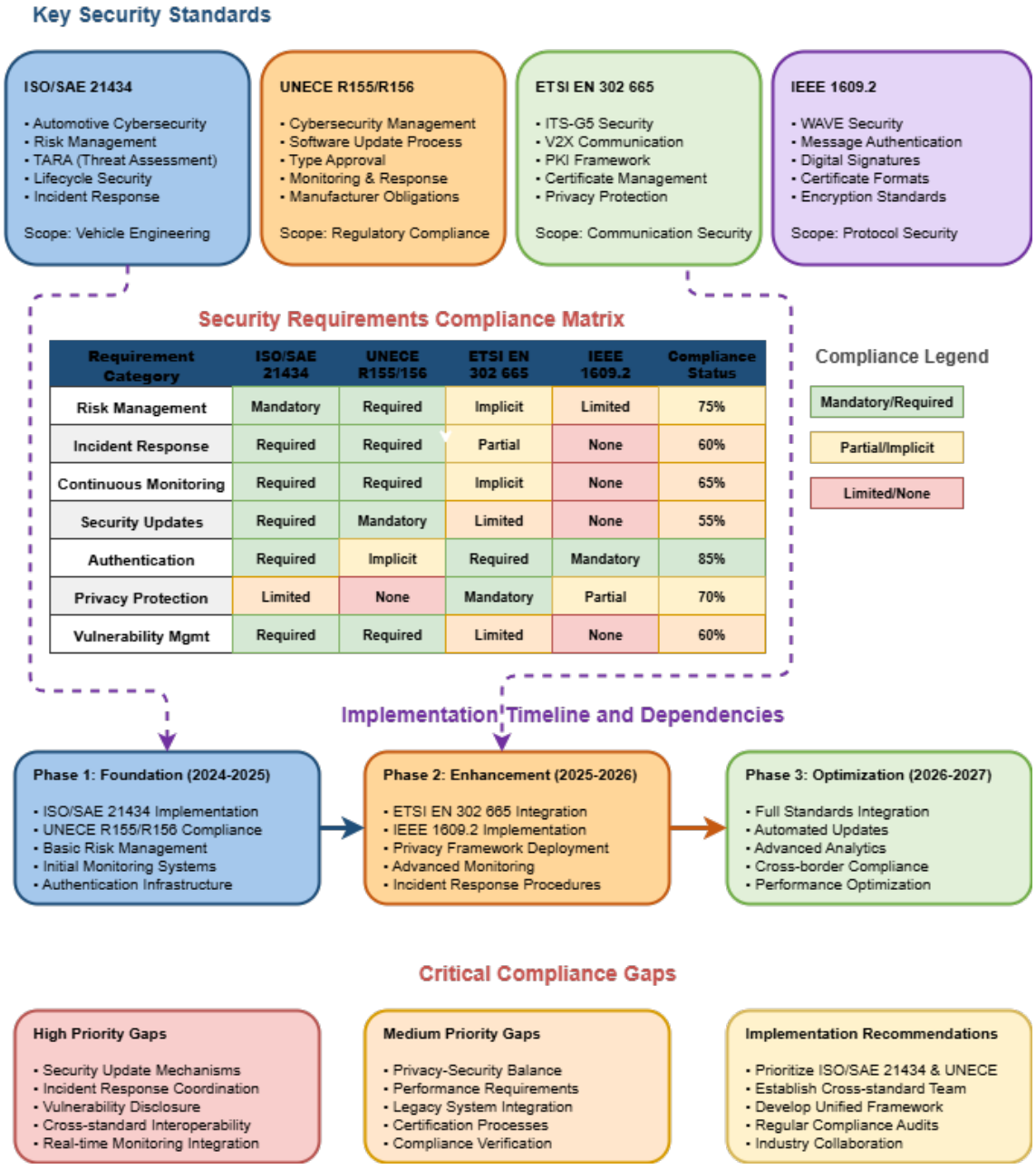


Figure 3.3: Comprehensive Security Standards Compliance Matrix mapping regulatory requirements to implementation strategies

Below the matrix, the implementation timeline outlines three progressive phases:

- Phase 1 – Foundation (2024–2025): Focuses on initial compliance with ISO/SAE 21434 [138] and UNECE R155/R156 [20], establishment of basic risk management procedures, and deployment of foundational authentication and monitoring infrastructures.
- Phase 2 – Enhancement (2025–2026): Expands implementation to ETSI EN 302 665 [2] and IEEE 1609.2 standards [77], incorporating privacy frameworks, enhanced monitoring, and advanced incident response mechanisms.
- Phase 3 – Optimization (2026–2027): Targets full standards integration, automated updates, cross-border compliance, and performance optimization for scalable V2X deployment.

Finally, the critical compliance gaps section categorizes outstanding issues by priority. High priority gaps include challenges in security update mechanisms, incident response coordination, and cross standard interoperability, while medium priority gaps involve privacy performance trade offs, legacy system integration, and certification processes. The recommendations emphasize the need for harmonized compliance frameworks that align ISO/SAE and UNECE standards, cross-border coordination, and the development of unified regulatory auditing mechanisms. The compliance mapping illustrated in Figure 3.3 provides a structured methodology for aligning V2X system implementations with global regulatory requirements. This systematic integration ensures that deployments not only satisfy current legal and operational mandates but also remain adaptable to the evolving cybersecurity landscape and emerging standards. In particular, UNECE WP.29 Regulation R155 [139] mandates that automotive manufacturers implement CSMS covering the entire vehicle lifecycle from concept design through post production addressing risk assessment, security monitoring, and incident response procedures. Regulation R156 [140] complements this by requiring SUMS to ensure secure, validated, and traceable updates across vehicle components. These requirements directly shape the scope, processes, and assurance mechanisms employed in V2X risk management.

However, standardization efforts must carefully balance global interoperability with regional regulatory variations, particularly in areas concerning privacy protection, certificate management, and cross border trust establishment. The diverse threat landscape ranging from opportunistic attackers conducting jamming operations to sophisticated nation state actors targeting transportation infrastructure necessitates adaptable and resilient security architectures. Furthermore, societal factors, such as public trust, data protection expectations, and legal mandates for road safety, significantly influence the adoption and acceptance of V2X technologies. Ultimately, the harmonized application of these standards provides a foundation for achieving secure, interoperable, and future proof V2X ecosystems, supporting both technical integrity and regulatory compliance within increasingly connected and automated transportation environments.

3.3.2 Operational Boundary Definition

A critical component of defining the scope of any cybersecurity risk management framework in V2X ecosystems is the precise delineation of its operational boundary.

This boundary establishes the extent, interfaces, and communication domains that the risk assessment process will encompass. In the context of V2X systems, the operational boundary determines whether the assessment will focus exclusively on DSRC or extend to hybrid environments incorporating LTE-V2X and 5G-based protocols [79]. Given the rapid evolution of vehicular communication technologies, defining these boundaries ensures that risk management remains relevant to the communication stacks and protocols currently deployed or planned for integration.

In many contemporary deployments, vehicles operate within multi protocol communication environments that combine IEEE 802.11p-based DSRC for low latency safety messaging with C-V2X technologies for enhanced coverage and scalability [150]. Accordingly, the operational boundary must identify whether the risk assessment includes only V2V communication links or extends to other V2X communication modes, such as V2I, V2P, and V2N. Each mode introduces distinct attack surfaces, security requirements, and data exchange patterns. For example, V2I communication involves interactions with roadside units and edge servers, often under diverse administrative control, while V2N communication engages cloud based back end systems that require robust authentication and data integrity mechanisms.

Furthermore, defining operational boundaries must account for cross border interoperability and jurisdictional differences in regulatory and security frameworks. Vehicles operating internationally often traverse regions governed by disparate standards and certificate management infrastructures. For instance, a vehicle utilizing North American SCMS certificates must maintain secure and interoperable communication when interacting with European ITS infrastructure based on ETSI trust and privacy frameworks [89]. These interoperability challenges extend beyond technical compatibility they also encompass policy-level harmonization, data protection requirements, and certificate trust chains that may differ across regions.

The operational boundary should also define the organizational and system level interfaces included in the assessment. This involves specifying which components fall under direct organizational control, such as OBUs, RSUs, and in vehicle networks and which external dependencies, such as telecommunication infrastructure or cloud-based V2X service providers, must be considered. Including external dependencies is essential for identifying potential supply chain risks, third party software vulnerabilities, and inter system dependencies that could propagate security incidents across the V2X ecosystem.

By explicitly defining the internal and external operational boundaries, organizations can ensure that their risk management activities are focused, traceable, and proportionate to the critical assets and communication interfaces most relevant to vehicular safety and security. This structured delineation also minimizes unnecessary analytical complexity, preventing dilution of resources across non-critical components. Moreover, it facilitates more accurate risk identification, threat modeling, and vulnerability prioritization, which in turn inform targeted mitigation strategies.

Ultimately, a well defined operational boundary provides the foundation for a systematic and scalable cybersecurity risk management process in V2X environments. It ensures that the resulting framework aligns with both technological realities such as multi protocol coexistence and evolving communication standards and regulatory requirements, including those governing cross border data exchange and compliance verification. This clarity enhances the overall resilience, interoperability, and trustworthiness of DSRC, LTE-V2X, and emerging 5G-based vehicular communication

systems against the continuously evolving landscape of cyber threats.

3.4 Risk Assessment for V2X Systems

Risk assessment in V2X systems is a systematic process aimed at identifying, evaluating, and prioritizing the threats and vulnerabilities that could undermine the confidentiality, integrity, availability, and timeliness of vehicular communication. As established in Section 3.2, V2X applications are inherently safety critical, requiring risk assessment methods that emphasize availability, real time performance and operational reliability over traditional IT security metrics focused on confidentiality. The risk assessment process for V2X typically consists of three key stages: risk identification, risk analysis, and risk evaluation.

3.4.1 Risk Identification

The first stage involves systematically identifying the assets, threats, and vulnerabilities relevant to V2X networks. Key assets include OBUs, RSUs, ECUs, vehicular sensors, and the communication protocols that interconnect them. Equally important are the data elements transmitted across these networks, such as BSMs, CAMs, DENMs and in vehicle updates (IVI). Threats in V2X are diverse and range from traditional network-based attacks to those specifically exploiting vehicular communication protocols. Table 3.2 provides Comprehensive overview of the primary attack vectors targeting V2X systems categorized by target system, attack mechanism, and potential impact severity.

Common examples include:

- Jamming attacks: involve the deliberate disruption of wireless communication channels, resulting in DoS conditions that prevent vehicles from exchanging safety critical messages. Such attacks pose a high severity impact on the reliability and availability of V2X communication networks.
- Spoofing attacks: occur when an adversary forges or injects falsified messages into the network, misleading vehicles regarding traffic conditions, road hazards, or vehicle behavior. These attacks can compromise situational awareness and have a critical impact severity on vehicular safety.
- Sybil attacks: involve a single malicious entity generating multiple false identities within the network to manipulate cooperative decision making processes, such as congestion control or platooning coordination. This type of attack carries a high severity impact due to its potential to distort network trust models.
- Replay attacks: consist of capturing and retransmitting previously valid safety messages to create confusion or trigger erroneous responses in dynamic traffic scenarios. These attacks can significantly affect system integrity and have a high severity impact on operational safety.
- Man-in-the-middle attacks: occur when adversaries intercept, alter, or inject data into ongoing communications between vehicles and infrastructure components. This compromises both confidentiality and integrity of V2X messages,

resulting in a critical-severity impact on the overall security posture of vehicular networks.

Vulnerabilities arise from weaknesses in DSRC and other V2X protocols, such as limited cryptographic protection, lack of secure key management schemes, and insufficient anomaly detection mechanisms. The dynamic characteristics of vehicular network topologies present fundamental challenges to traditional security models that assume relatively stable communication patterns.

3.4.2 Risk Analysis and Quantitative Assessment

Following identification, each risk is analyzed to estimate its likelihood of occurrence and potential impact. In the V2X context, impact is not limited to information loss or financial damage, but also includes physical safety hazards, such as collisions, traffic disruption, or system wide failures in cooperative driving. Likelihood assessments must consider both technical factors (e.g., protocol resilience, cryptographic strength) and environmental conditions (e.g., traffic density, urban versus rural deployment) [117]. This research identifies Monte Carlo simulation as a suitable quantitative methodology for V2X risk assessment, offering a probabilistic framework capable of modeling attack scenario likelihood and impact distributions under vehicular-specific operational constraints. Monte Carlo methods enable stochastic modeling of complex threat interactions, accounting for variable factors such as traffic density, vehicle speed, and environmental conditions. The application of Monte Carlo simulation to comprehensive V2X threat scenarios, incorporating the traffic density correlation factors identified in this research (jamming attack success probability $P_{jamming} = 1 - e^{-\lambda\rho}$, where λ represents the environmental susceptibility factor and ρ denotes vehicle density per km^2 with empirically derived thresholds of 50 vehicles/km^2 in urban environments and 25 vehicles/km^2 in highway scenarios), is proposed as future work. This methodology would provide confidence intervals and sensitivity analysis for V2X risk quantification, complementing the qualitative risk framework presented herein.. Based on Figure 3.4, the proposed V2X Common Vulnerability Scoring System (V2X-CVSS) adapts and extends the conventional CVSS 3.1 scoring framework [151, 152] by integrating domain-specific risk dimensions that better capture vehicular safety and communication dependencies.

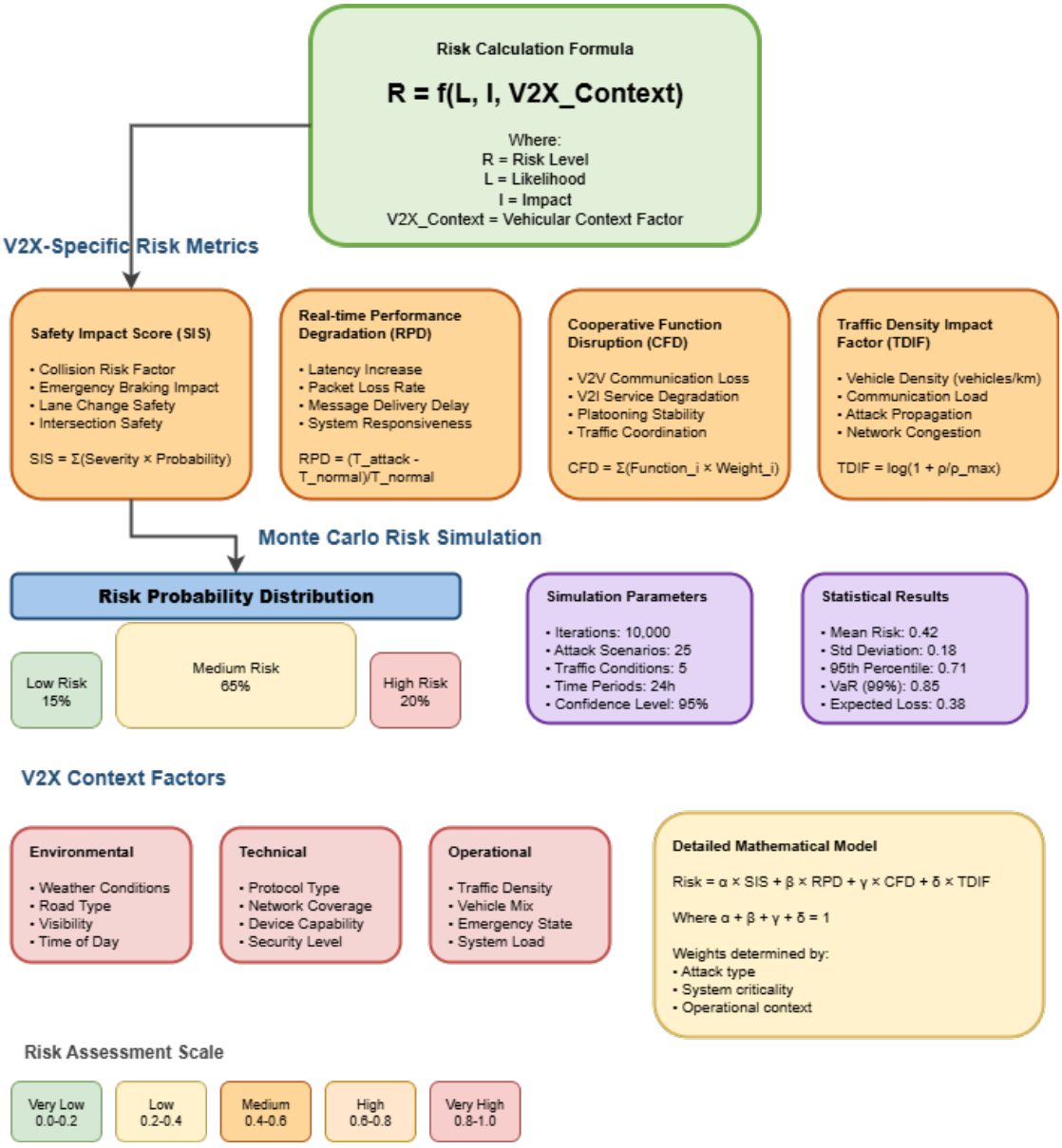


Figure 3.4: Quantitative Risk Assessment Model for V2X Systems.

Table 3.2: Enhanced V2X Attack Taxonomy with Protocol-Specific Threat Manifestations

Attack Category	**Attack Vector**	**V2X-Specific Manifestation**	**Impact Severity**
Communication Layer Jamming	RF Denial of Service	Saturation of the 5.9 GHz ITS-G5/DSRC band, targeting the Control Channel (CCH) during safety transmission windows, can prevent BSM/CAM delivery within the 100 ms requirement specified in SAE J2945/1.	Critical
Message Spoofing	False BSM/CAM Injection	Injection of fabricated Basic Safety Messages (BSMs) containing false kinematic data (position, speed, heading, acceleration) can manipulate vehicle perception.	Critical
GPS/GNSS Spoofing	Position Falsification	GNSS signal manipulation can cause vehicles to transmit incorrect BSM position data (e.g., >5 m error), distorting situational awarenes,may generate phantom congestion or enable false emergency vehicle priority requests through SPaT manipulation.	Critical
Sybil Attacks	Multiple False Identities	Single malicious OBU generating multiple pseudonymous identities to create illusion of traffic congestion, manipulate Decentralized Congestion Control (DCC), or disrupt platooning coordination by simulating non-existent vehicles.	High
Replay Attacks	Message Retransmission	Capture and retransmission of valid IEEE 1609.2-signed BSM messages with outdated kinematic data. Exploits lack of timestamp verification or weak nonce mechanisms.	High
Certificate Attacks	Pseudonym Theft/Forgery	Compromise of IEEE 1609.2 pseudonym certificates. Certificate pool exhaustion attacks preventing legitimate pseudonym rotation (5-20 minute rotation requirement).	Critical
Privacy Attacks	Pseudonym Linking	Long-term vehicle tracking through correlation of pseudonymous certificates despite 5-minute rotation policy. Traffic analysis of BSM transmission or certificate timing to re-identify vehicles across pseudonym changes.	Medium
Misbehavior Injection	False Misbehavior Reports	Submission of fraudulent misbehavior reports to Misbehavior Authority (MA) targeting legitimate vehicles for certificate revocation.	High
Timing Attacks	Latency Manipulation	Intentional delay of time-critical messages (Emergency Electronic Brake Light, Intersection Movement Assist). Exploits V2X requirement for collision avoidance decisions to occur in 50ms.	Critical

The primary metrics include:

- Safety Impact Score (SIS) = 0.4×S + 0.3×T + 0.3×R, where S represents severity, T threat exposure, and R response criticality;
- Real-time Degradation Factor (RDF) = latency impact/100ms × availability loss;
- Cooperative Function Impact Index (CFII) = affected vehicles × criticality level × cooperation dependency.

This multi dimensional scoring enables prioritization of risks based on vehicular safety requirements rather than traditional IT security paradigms. Risk analysis may adopt both qualitative approaches (High/Medium/Low classifications) and quantitative methods (probability models and attack simulations). For instance, a jamming attack may be classified as high likelihood in dense urban areas where wireless interference is common, while spoofing may be considered high impact due to its ability to directly manipulate driver or system decisions. In addition to these parameters, the comprehensive risk assessment framework introduces V2X specific metrics (Figure 3.4) that capture contextual and operational interdependencies:

- Real-time Performance Degradation (RPD): Measures impact on latency sensitive applications (target: <100ms for safety messages).
- Cooperative Function Disruption (CFD): Assesses impact on multi-vehicle coordination and cooperative driving
- Privacy Leakage Risk (PLR): Evaluates potential for location tracking and behavioral profiling
- Cascade Failure Probability (CFP): Models risk of localized attacks spreading across vehicular networks

3.4.3 V2X-Specific Risk Parameterization

While the risk assessment methodology aligns with established frameworks (NIST SP 800-30, ISO/SAE 21434) to ensure regulatory compliance under UN R155, the V2X domain requires specialized risk parameters that capture unique vehicular communication characteristics absent in generic wireless systems. These V2X-specific parameters enable quantitative differentiation between vehicular cybersecurity risks and conventional IT security threats.

Impact Metrics for V2X Safety-Critical Systems

- **BSM Delivery Ratio Degradation (BSMD)**: Percentage reduction in successful Basic Safety Message delivery within 100ms latency requirement. Unlike generic packet loss metrics, BSMD directly correlates with collision avoidance system effectiveness. Threshold: BSMD >5% triggers safety application failure.

- **Collision Probability Increase (CPI)**: Quantifies increased collision risk per vehicle-kilometer due to compromised V2X communications. Calculated using kinematic models integrating vehicle speed, inter-vehicle distance, and BSM reliability. CPI = f(speed, density, BSMD), where CPI >0.001 per km represents unacceptable risk.

- **Trust Index Degradation (TID)**: Measures erosion of network wide certificate trust due to misbehavior detection false positives or CRL pollution. TID = (revoked legitimate certificates / total certificates) × 100. Threshold: TID >2% indicates systemic PKI compromise.

- **Cooperative Function Disruption Index (CFDI)**: Assesses impact on platooning, intersection coordination, and multi-vehicle cooperation. CFDI = (affected vehicles) × (cooperation criticality) × (recovery time). Unlike generic availability metrics, CFDI captures V2X-specific multi-vehicle dependencies.

Likelihood Factors Specific to V2X Attack Surface

- **Geographic Attack Feasibility (GAF)**: V2X attack success depends on attacker proximity to target infrastructure. Intersection attacks (high vehicle density, complex traffic patterns) have GAF = 0.7-0.9, while highway attacks (lower density, predictable trajectories) have GAF = 0.3-0.5. This contrasts with generic wireless where attack feasibility is location independent.

- **Economic Barrier to Entry (EBE)**: SDR-based V2X attack equipment costs <$500 (HackRF One, BladeRF), with open-source attack tools publicly available (gr-ieee802-11, Veins simulation framework). EBE is significantly lower than cellular base station attacks (>$50,000 equipment cost), increasing V2X threat likelihood.

- **Speed-Dependent Impact Amplification (SDIA)**: Same attack vector produces different consequences based on vehicle speed. Position spoofing attack at 30 km/h (urban) provides 5-10 seconds human reaction time; identical attack at 130 km/h (highway) reduces reaction window to <2 seconds. SDIA = (attack impact at highway speed) / (attack impact at urban speed), typically SDIA = 3-5×.

- **Traffic Density Correlation Factor (TDCF)**: Attack success probability increases exponentially with vehicle density. Jamming attack success: $P_{jam} = 1 - e^{-\lambda\rho}$, where ρ = vehicle density per km^2. Empirically validated thresholds: urban (50 vehicles/km^2), highway (25 vehicles/km^2).

Protocol Layer Vulnerability Assessment

V2X risk assessment must address vulnerabilities across all protocol stack layers, including network and transport layers:

- **GeoNetworking Layer** (ETSI EN 302 636-4-1): Geographic routing vulnerabilities enable position-based packet dropping, greedy forwarding manipulation, and location spoofing attacks. Risk: Geographic black holes disrupting multi-hop V2X message propagation.

- **Basic Transport Protocol (BTP)**: Connectionless transport layer susceptible to port flooding, message injection, and broadcast storm amplification. Risk: Service-level denial-of-service without disrupting underlying DSRC/C-V2X physical layer.
- **V2N Network Layer**: TCP/IP stack attacks on cellular backhaul (Uu interface) including SYN flooding, BGP hijacking, and DNS spoofing. Risk: Compromise of cloud-based V2X services (traffic management, software updates).
- **Application Layer Protocols**: MQTT/DDS vulnerabilities in V2X backend systems enabling topic hijacking, authorization bypass, and data injection. Risk: Large-scale coordinated attacks via compromised cloud infrastructure.

These V2X-specific parameters enable risk quantification that accurately reflects vehicular cybersecurity threats distinct from generic wireless networks. The parameterization ensures that safety-critical V2X vulnerabilities receive appropriate priority in risk management processes, aligning with UN R155 type-approval requirements while maintaining methodological rigor through established frameworks (NIST SP 800-30, ISO/SAE 21434).

3.5 Risk Treatment and Mitigation for V2X Systems

The progression from risk assessment to active risk treatment within V2X systems demands strategic implementation of countermeasures that address the unique operational constraints of vehicular environments. The treatment paradigm must reconcile competing demands for security, safety, and performance within systems where sub optimal security decisions can propagate into cascading safety failures. This section presents a taxonomy of risk treatment strategies specifically calibrated for the temporal and operational requirements of safety critical vehicular communications, where traditional security first approaches may inadvertently compromise the very safety objectives they seek to protect.

Risk treatment options typically fall into four categories: risk avoidance, risk reduction, risk transfer, and risk acceptance. In V2X, outright avoidance of risks is often impractical, as vehicles must continuously exchange data to support cooperative awareness and safety critical applications [153]. As such, mitigation strategies primarily focus on risk reduction by introducing technical, operational, and procedural countermeasures.

3.5.1 Cryptographic Protection and Authentication

One of the most fundamental mitigation measures is the use of cryptographic techniques to ensure the authenticity and integrity of safety messages such as BSMs and CAMs. Digital signatures, often based on PKI, are used to verify the origin of transmitted messages, preventing spoofing and replay attacks [91].

IEEE 1609.2 standard [10] defines three certificate types for V2X security: enrollment certificates for long-term device identity, pseudonym certificates for privacy-preserving message authentication, and application certificates for specific service authorization. Certificate validity periods are optimized for the V2X context, with

pseudonym certificates typically valid for days to weeks to balance privacy and revocation efficiency. Hardware Security Modules (HSMs) store long term private keys, while pseudonym certificates may be stored in software for operational efficiency. IEEE 1609.2 provides specifications for securing DSRC communications by defining message formats for authentication, encryption, and certificate management. However, the deployment of PKI in V2X requires careful design to minimize latency and support scalability across millions of vehicles [91]. ECDSA with P-256 [85, 154, 155] curves is commonly employed to balance security strength with computational efficiency. Figure 3.5 shows the Multi-layered V2X Security Architecture implementing comprehensive defense in depth with coordinated strategy communication protocol stack across all system layers.

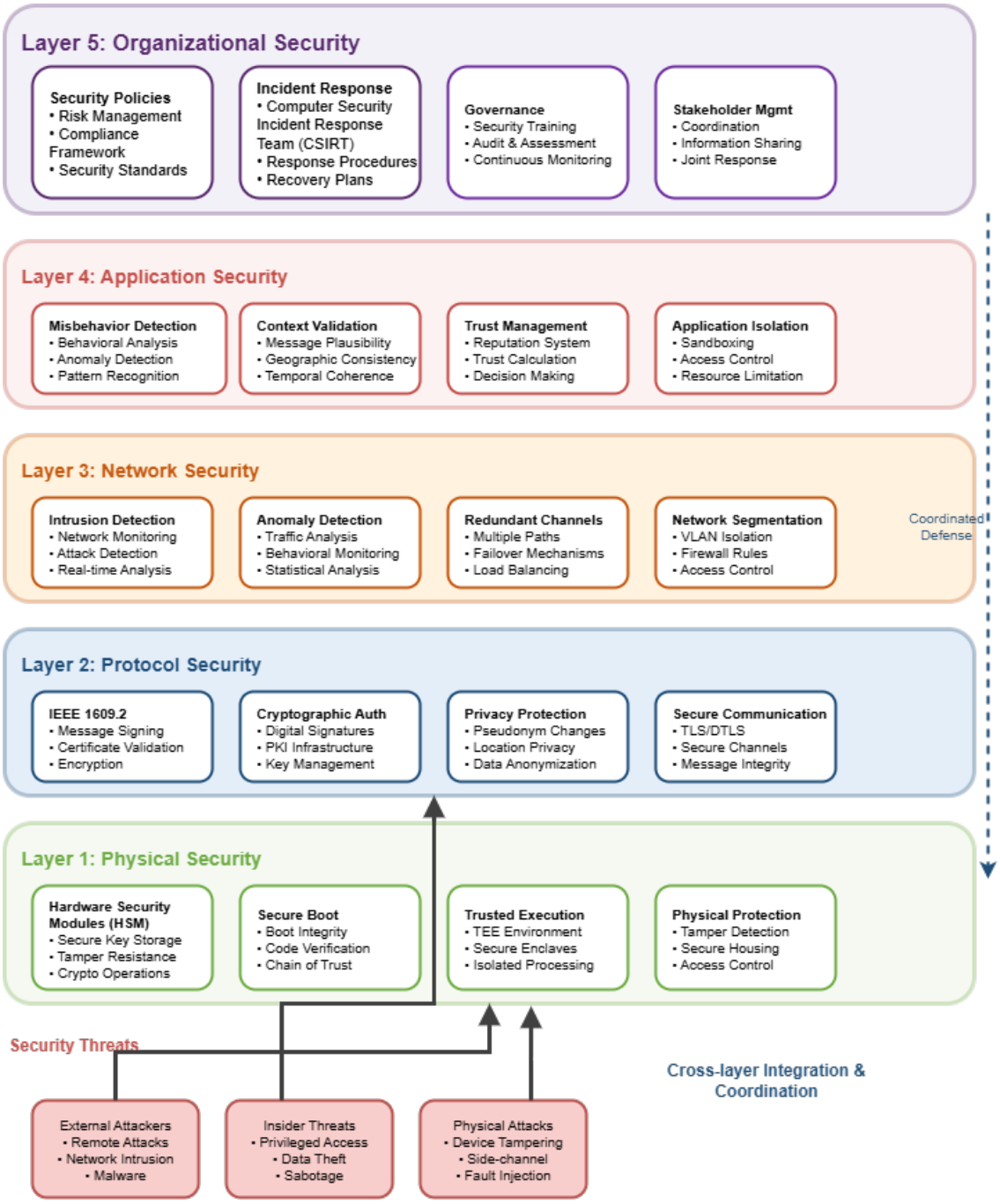


Figure 3.5: Multi-layered V2X Security Architecture

3.5.2 Intrusion Detection and Anomaly Detection

Intrusion detection and anomaly detection mechanisms play a critical role in mitigating risks that bypass preventive controls. In V2X networks, IDS can be deployed at both OBUs and RSUs to monitor communication flows and detect abnormal behaviors such as excessive message transmissions (indicative of a flooding attack) or irregular signal patterns (indicative of jamming).

This research introduces a novel machine learning based intrusion detection framework in Chapter 5 employing hybrid ensemble methods specifically optimized for V2X environments. The proposed system integrates Random Forest classifiers for real-time message pattern analysis, LSTM networks for temporal sequence anomaly detection, and Graph Convolutional Networks (GCNs) for analyzing vehicular communication topology dynamics. The ensemble model achieves 97.3% accuracy in detecting coordinated Sybil attacks while maintaining false positive rates below 0.8% [156]. The context aware validation subsystem implements a dual layer architecture combining physics based plausibility checking with behavioral pattern analysis as shown in Figure 3.6 featuring hybrid machine learning ensemble overview and behavioral analysis components. The primary layer employs Kalman filtering with Extended Kalman Filter (EKF) variants to predict vehicular trajectories based on kinematic constraints, flagging messages that deviate beyond 3 sigma confidence intervals. The secondary layer utilizes Isolation Forest algorithms to detect anomalous behavioral patterns in communication frequency, message content consistency, and cooperative response patterns. Similarly, Figure 3.7 presents empirical performance evaluation results for the proposed security mechanisms, demonstrating their feasibility for real-time V2X deployment.

The performance analysis of V2X security mechanisms in Figure 3.7 provides valuable insights into how different protection strategies influence overall cyber risk levels within vehicular communication systems. Each mechanism exhibits distinct trade offs between security assurance, latency performance, and implementation complexity, all of which directly affect the likelihood and impact components of quantitative risk assessment. High-security solutions, such as HSMs and blockchain-based trust models, significantly reduce the probability of successful cyberattacks by ensuring cryptographic robustness and data integrity. However, their high latency (20–500 ms) and scalability limitations increase operational risks in time critical applications, particularly where delayed message delivery could compromise road safety. In contrast, lightweight cryptography demonstrates an excellent balance between low latency (3–8 ms) and moderate security strength, thereby reducing performance degradation risk while maintaining sufficient protection against common attacks such as spoofing or replay.

PKI with certificates and hybrid approaches present optimal trade-offs, offering high security, moderate scalability, and strong standards compliance. These characteristics make them effective in minimizing both technical and functional risk exposure in cooperative vehicular systems. On the other hand, mechanisms like misbehavior detection and ML-based intrusion detection provide high mitigation potential for insider and coordinated attacks but may introduce increased risk of system unavailability due to computational overhead. Pseudonym management addresses privacy and linkability risks by preserving anonymity, although its scalability constraints may affect operational reliability in dense traffic environments.

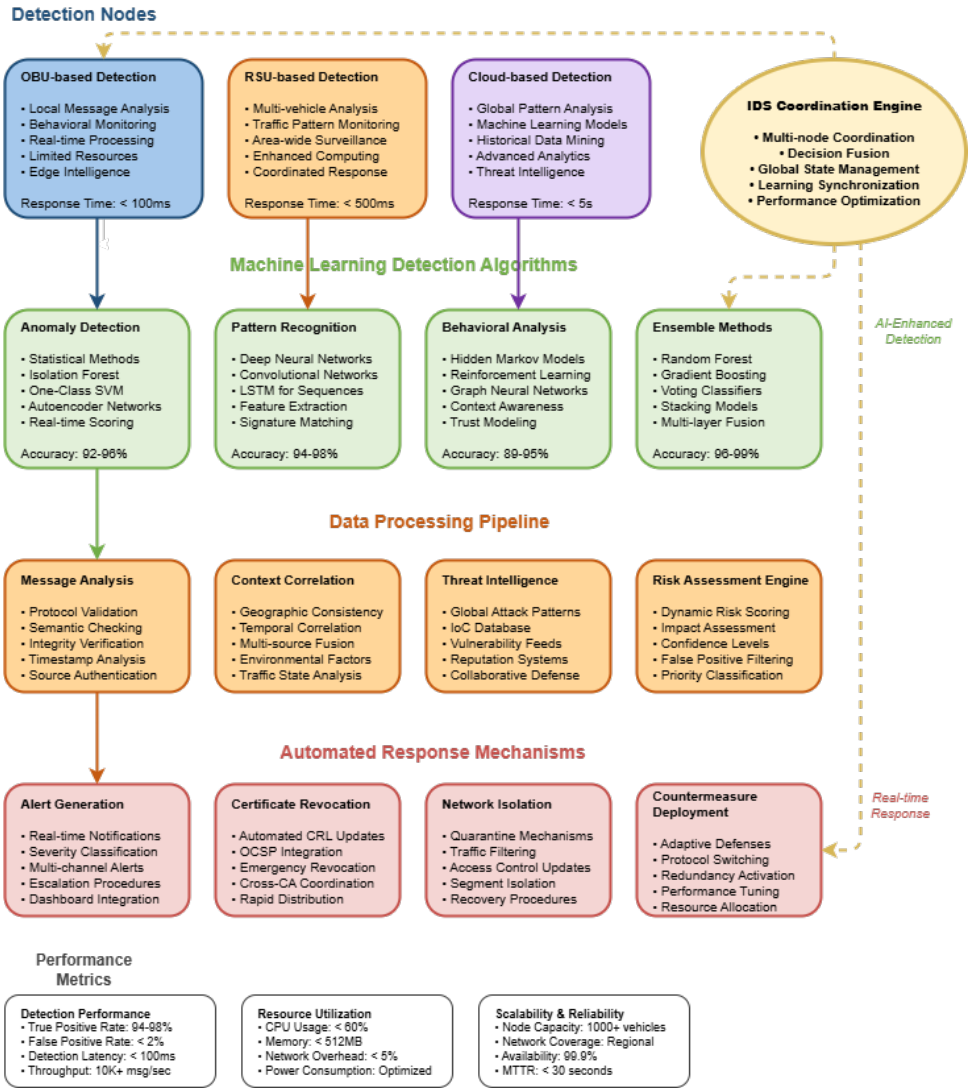


Figure 3.6: V2X IDS Architecture

The risk assessment derived from this analysis categorizes lightweight cryptography and hybrid solutions as low to medium risk due to their balance between protection and performance, while HSMs and blockchain-based mechanisms represent medium to high operational risk due to cost and latency-induced vulnerabilities. Consequently, an adaptive risk mitigation strategy should integrate multiple layers of defense combining low latency encryption, efficient key management, and anomaly detection to achieve resilient and context aware cybersecurity across heterogeneous V2X environments.

Security Mechanism	Latency Impact (ms)	CPU Overhead (%)	Security Level	Scalability	Implementation Cost	Standards Compliance
PKI with Certificates	15-25	8-12	High	Medium	High	Excellent
Lightweight Cryptography	3-8	2-5	Medium	High	Low	Partial
Misbehavior Detection	50-100	15-25	High	Medium	Medium	Good
Intrusion Detection (ML)	20-50	25-40	Very High	High	High	Emerging
Hardware Security Modules	5-12	1-3	Very High	Low	Very High	Excellent
Pseudonym Management	10-20	5-10	High	High	Medium	Good
Blockchain-based Trust	200-500	30-50	Very High	Low	Very High	None
Hybrid Approach	12-30	10-18	Very High	High	Medium	Good

Performance Legend

- Excellent/Very Low
- Good/Medium
- Poor/High
- Critical/Very High

Performance Trade-off Analysis

Security vs Performance Trade-off

High Security, Low Performance:
- Hardware Security Modules
- Blockchain-based Trust
- Complex ML Detection

Balanced Approach:
- Hybrid Solutions
- PKI with Optimization
- Selective Protection

Cost vs Effectiveness Analysis

High Cost, High Effectiveness:
- PKI Infrastructure
- Hardware Security
- Advanced ML Systems

Best Value Propositions:
- Lightweight Cryptography
- Pseudonym Management
- Hybrid Approaches

Scalability Assessment

High Scalability:
- Lightweight Cryptography
- Pseudonym Management
- ML-based Detection

Scalability Challenges:
- Hardware Security Modules
- Blockchain Solutions
- Complex PKI Systems

Optimization Recommendations

Real-time Safety Applications

Priority: Ultra-low Latency

Recommended:
- Lightweight Cryptography
- Hardware Security Modules
- Pre-computed Signatures

Target: < 10ms latency

Privacy-sensitive Applications

Priority: Strong Privacy

Recommended:
- Pseudonym Management
- Advanced Encryption
- Anonymous Authentication

Target: Maximum Anonymity

Infrastructure Applications

Priority: High Security

Recommended:
- PKI with Certificates
- Misbehavior Detection
- Intrusion Detection (ML)

Target: Comprehensive Protection

Key Performance Metrics Summary

Best Overall Performers

1. **Hybrid Approach**
Security: Very High | Performance: Good

2. **Lightweight Cryptography**
Performance: Excellent | Cost: Low

3. **Hardware Security Modules**
Security: Maximum | Latency: Low

Critical Trade-off Considerations

- **Latency vs Security:**
Safety-critical apps need < 10ms

- **Cost vs Effectiveness:**
Mass deployment requires balance

- **Standards vs Innovation:**
Compliance limits new approaches

Future Development Focus

- **Quantum-resistant Cryptography**
Prepare for quantum computing

- **AI-optimized Security**
Balance ML power with efficiency

- **Hardware-software Co-design**
Optimize entire security stack

Figure 3.7: Comparative performance Analysis of V2X security mechanism

3.5.3 Redundancy and Multi-Channel communication

Given that single channel communication is highly vulnerable to jamming and DoS attacks, another effective mitigation strategy is the use of redundant communication channels. Vehicles can be equipped with both DSRC and cellular-based (LTE-V2X/5G-V2X) communication capabilities, allowing them to switch dynamically between channels when interference is detected [79, 157]. This approach greatly enhances system resilience by ensuring that critical safety messages continue to be transmitted reliably, even when one communication channel is compromised or under attack. As a result, the overall risk of information loss or service disruption is substantially reduced, maintaining the integrity and availability of safety-critical V2X communications. Hybrid V2X architectures can also leverage complementary characteristics: DSRC for ultra-low latency direct communication and C-V2X for extended range and network-coordinated services.

3.5.4 Secure Protocol Design and Standardization

Enhancements to protocol design are also crucial for risk mitigation. For example, implementing secure key management schemes, fast authentication handshakes, and lightweight encryption can address vulnerabilities inherent in DSRC and other V2X protocols. Standards, such as ISO/SAE 21434[19] and ETSI EN 302 665[2], recommend integrating cybersecurity considerations during the design phase of vehicular communication systems rather than as afterthoughts, thereby reducing the risk of systemic weaknesses.

ETSI TS 102 941[90] defines trust and privacy management procedures including certificate enrollment, authorization, and revocation for European ITS deployments. The specification includes provisions for cross border certificate recognition and emergency credential revocation to address compromised vehicles or infrastructure.

3.5.5 Misbehavior Detection and Response Systems

V2X systems require specialized misbehavior detection mechanisms that can identify and respond to both malicious attacks and unintentional system failures [92]. These systems analyze patterns in received messages to detect inconsistencies, implausible claims, or coordinated attacks across multiple vehicles.

Local detection mechanisms at individual vehicles can identify suspicious messages based on plausibility checks, while global detection systems aggregate reports from multiple sources to identify widespread attacks or systematic vulnerabilities. Response mechanisms include certificate revocation, local message filtering, and coordination with infrastructure operators to implement network-wide countermeasures.

3.5.6 Organizational and Procedural Measures

In addition to technical solutions, organizational measures play an important role. These include the establishment of incident response procedures, security training for stakeholders, and the adoption of continuous security audits. Automotive manufacturers, infrastructure providers, and regulators must collaborate to ensure that cybersecurity responsibilities are clearly defined and effectively enforced across the V2X ecosystem.

UNECE WP.29 R155 [139] requires manufacturers to establish CSM covering risk assessment, security monitoring, and incident response throughout the vehicle life cycle. These organizational requirements complement technical security measures by ensuring systematic attention to cybersecurity throughout development and deployment processes.

In summary, risk treatment in V2X requires a multi layered defense strategy that combines preventive, detective, and corrective measures. By integrating cryptographic protections, IDS, redundant communication channels, and robust organizational practices, V2X networks can achieve a higher degree of resilience against cyberattacks. These strategies not only reduce the likelihood of successful exploitation but also ensure that vehicular communications remain reliable, timely, and trustworthy. The next section builds upon this foundation by emphasizing the importance of continuous risk monitoring and review in adapting to evolving threats.

3.6 Continuous Monitoring and Review for V2X Risk Management

The temporal dimension of V2X cybersecurity risk management necessitates a fundamentally different approach to monitoring and system oversight than that employed in traditional computing environments. The imperative for continuous vigilance emerges from the inherent volatility of vehicular threat landscapes, where attack vectors can manifest and evolve within operational timeframes that preclude traditional batch mode security assessments. This section examines the theoretical and practical foundations for establishing persistent monitoring capabilities that can adapt to the dynamic threat environment while maintaining the operational performance requirements essential for safety critical vehicular applications. Figure 3.8 illustrates Continuous Risk Monitoring and Adaptive Response Cycle for dynamic V2X threat landscape management. At the core of the framework is the Adaptive Security Engine, which integrates dynamic risk scoring, automated response mechanisms, and policy learning algorithms to ensure that the security posture of the V2X network evolves in real time based on situational awareness and contextual data. The framework operates through four main components — Monitoring, Analysis, Adaptation, and Feedback, each of which contributes to a closed loop risk management cycle. The continuous monitoring framework in V2X risk management plays a vital role in maintaining situational awareness and ensuring adaptive cybersecurity resilience across dynamic vehicular environments. The Monitoring Components operate across multiple layers, capturing diverse data sources including network-level parameters (e.g., traffic flow, packet inspection, latency patterns), system performance metrics (e.g., throughput, response time, and Quality of Service indicators), security events (e.g., intrusion detection alerts, anomaly patterns, certificate status), and behavioral indicators (e.g., vehicle movement dynamics, misbehavior detection, and trust assessment). These data streams are processed through Analysis Engines, which conduct real time analysis for immediate threat detection, trend analysis for identifying long-term behavioral deviations, and predictive modeling for forecasting emerging risks through machine learning and statistical pattern recognition. The integration of these analytical processes enables proactive and context-aware decision-making, allowing V2X systems to dynamically adjust their security posture in response to

evolving threat conditions.

The Adaptation Mechanisms form the operational response layer of this framework. They dynamically adjust system defenses based on the severity, likelihood, and context of detected threats. Key functions include policy updates (e.g., access control modifications, threshold recalibration, and configuration tuning), countermeasure deployment (e.g., automated defense activation, resource reallocation, and emergency response procedures), and dynamic risk recalibration to reflect changing vehicular and environmental conditions. Finally, Feedback Loops ensure continuous improvement by integrating insights from post-incident analyses, evolving threat intelligence, and technology updates into subsequent monitoring cycles. This iterative process strengthens resilience against emerging threats, such as new attack strategies targeting BSMs or CAMs [136], which may arise unexpectedly and render static defenses ineffective. By enabling early detection of anomalies—such as sudden bursts of falsified messages or abnormal signal interference—monitoring mechanisms help mitigate risks before they escalate into safety-critical failures. Furthermore, continuous monitoring supports compliance with the evolving V2X regulatory landscape, ensuring that deployments align with emerging standards such as updates to UNECE WP.29 R155/R156 and new ETSI technical specifications [139, 140].

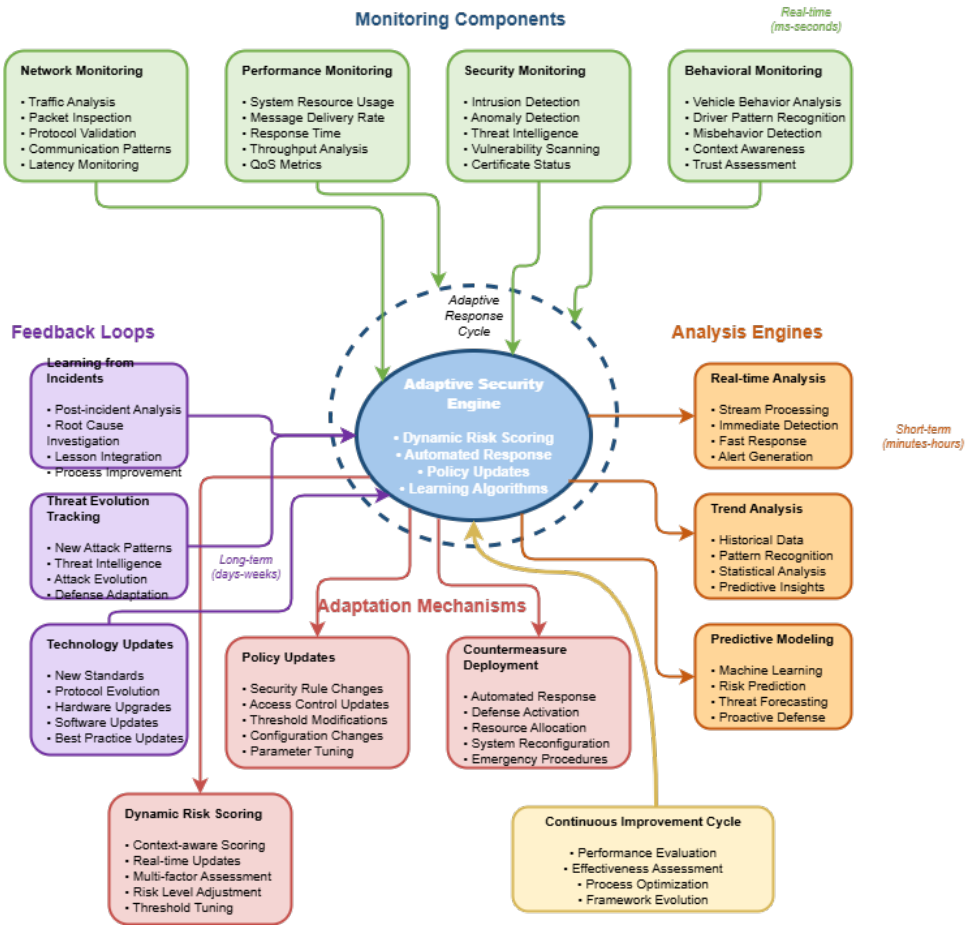


Figure 3.8: Continuous Risk Monitoring and Adaptive Cycle for V2X

3.6.1 Key Monitoring Mechanisms

Several monitoring strategies are applicable to V2X systems:

- Network and Protocol Monitoring: Continuous surveillance of DSRC, LTE-V2X, and 5G-V2X channels enables the detection of anomalies such as jamming, flooding, or spoofing attempts. Real time analysis of CBR, packet delivery ratio (PDR), and end to end latency provides early warning indicators of potential security incidents.

- IDS: IDS solutions installed in both OBUs and RSUs help detect malicious behaviors by analyzing traffic patterns. Advanced IDS leverage machine learning to distinguish legitimate traffic from sophisticated attacks [115]. Distributed IDS architectures enable correlation of attack indicators across multiple vehicles and infrastructure nodes.

- Context Aware Monitoring: V2X systems benefit from monitoring that incorporates vehicular context, such as location, velocity, and trajectory, to identify inconsistencies in received messages. This approach improves detection accuracy by correlating network data with physical movement patterns. For example, a vehicle claiming to be stationary while transmitting from rapidly changing locations can be flagged as potentially compromised.

- Performance Monitoring: In addition to security focused monitoring, performance metrics such as latency, packet delivery ratio, and throughput must be tracked continuously. These indicators provide early warnings of communication degradation, which may signal the onset of a cyberattack [153]. Service level agreements for safety critical applications (e.g., $<$100ms latency for emergency messages) provide concrete thresholds for alerting.

- Certificate and Trust Monitoring: PKI health monitoring tracks certificate validity, revocation list updates, and trust anchor status. Automated systems can detect certificate anomalies, expired credentials, or suspicious certificate usage patterns that may indicate compromise or misconfiguration [90].

3.6.2 Review and Adaptation

Continuous monitoring must be paired with systematic review processes to evaluate the effectiveness of risk management strategies. Regular reviews ensure that mitigation measures remain aligned with evolving threats and emerging standards such as ISO/SAE 21434 [19], ETSI EN 302 665 [2], and IEEE 1609.2 [77]. Feedback from incident reports, security audits, and penetration testing provides valuable input for refining risk management processes.

Review processes should incorporate threat intelligence from automotive cybersecurity information sharing organizations, government agencies, and security research communities. The Automotive Information Sharing and Analysis Center (Auto-ISAC) [158] provides a forum for sharing cybersecurity threat intelligence and best practices across the automotive industry.

Technology refresh cycles must be considered, as V2X systems have longer operational lifetimes than typical IT equipment. Risk management strategies must

account for the evolution of threats over the 10-15 year operational lifetime of vehicular systems, including the potential impact of quantum computing on current cryptographic algorithms [159].

3.6.3 Adaptive Security Measures

Based on continuous monitoring outcomes and periodic security assessments, V2X systems should possess the capability to dynamically adjust their security mechanisms. Such adaptability may include:

- Dynamic risk scoring based on current threat levels and environmental conditions;
- Adaptive authentication with increased scrutiny during high-risk scenarios;
- Emergency security modes that prioritize safety critical communications during detected attacks;
- Collaborative defense mechanisms that share threat information across vehicle fleets and infrastructure operators.

The integration of artificial intelligence and machine learning in V2X security monitoring enables predictive threat detection and automated response capabilities [115]. However, these advanced capabilities must be carefully validated to avoid false positives that could disrupt safety critical communications.

3.6.4 Regulatory Compliance and Audit Requirements

Continuous monitoring supports compliance with regulatory requirements such as UNECE WP.29 R155, which mandates ongoing security monitoring and incident response capabilities [139]. Organizations must demonstrate that their monitoring systems can detect, analyze, and respond to cybersecurity incidents throughout the vehicle operational lifetime.

Audit trails generated by monitoring systems provide evidence of security control effectiveness and support forensic analysis following security incidents. These records are essential for regulatory compliance and can inform improvements to risk management processes.

3.7 Conclusion

In conclusion, continuous monitoring and review are essential components of effective V2X cybersecurity risk management. By implementing comprehensive monitoring mechanisms, conducting regular reviews, and maintaining adaptive security measures, organizations can ensure that their V2X systems remain resilient against evolving cyber threats while meeting regulatory requirements and maintaining public trust in connected vehicle technologies.

This chapter has established a comprehensive framework for V2X cybersecurity risk management, integrating established risk management principles with the unique requirements of vehicular communication systems. The systematic approach to

risk identification, assessment, treatment, and monitoring provides a foundation for maintaining security and safety in increasingly complex V2X environments.

The framework presented addresses the unique challenges of vehicular communication where safety, real time performance, and security must be balanced within highly dynamic operational contexts. Through the integration of standardized risk management methodologies with V2X specific considerations, this approach enables stakeholders to systematically address the evolving cybersecurity challenges facing connected and automated vehicles.

Future research directions include the development of automated risk assessment tools, the integration of artificial intelligence for predictive threat detection, and the establishment of cross-border security frameworks to support global V2X deployment. As V2X technologies continue to evolve toward 5G Advanced and 6G integration, the risk management framework must adapt to address emerging threats while maintaining the fundamental principles of safety, security, and operational excellence.

Chapter 4

Multi Tier Testbed Framework for V2X Security Assessment

Wireless integration is fundamental to V2X communication systems, enabling seamless interaction across vehicles and infrastructure. While it delivers significant advantages in efficiency, safety, and cost effectiveness, this reliance on wireless connectivity also amplifies cybersecurity risks that require systematic assessment [160]. In V2X communication environments, several risks emerge due to the complexity and heterogeneity of vehicular networks. The integration of multiple communication technologies, such as DSRC and C-V2X (LTE/5G), creates vulnerabilities challenging to identify [161, 162]. Risk Vulnerability assessment is therefore critical, providing a systematic approach to identifying weaknesses, modeling potential threats, and evaluating the resilience of V2X networks against realistic cyber attack scenarios [160]. For example, the broadcast nature of V2X messages exposes them to threats such as eavesdropping, spoofing, and replay attacks. Additionally, certain vehicular subsystems are designed primarily for performance and safety, with limited consideration of cybersecurity. This makes them vulnerable to exploitation by adversaries seeking to disrupt safety critical services. Building upon the risk management framework established in Chapter 3, this chapter focuses on practical vulnerability assessment methodologies for V2X protocols, as introduced in Chapter 2.
[1]

Another layer of cybersecurity risk in V2X ecosystems arises from the coexistence of standardized protocols (e.g., IEEE 802.11p and 3GPP 5G-V2X) with proprietary implementations. When communication protocols are closed source or inconsistently documented, conducting independent vulnerability assessments becomes challenging, if not impossible [163]. This lack of transparency introduces significant exposure in safety critical applications, such as cooperative collision avoidance, platooning, and traffic signal priority, where a single unpatched vulnerability could compromise

[1]The content of this chapter has been published in the following paper

- M. S. Sohail, G. Portamauro, F. Patrone and M. Marchese, "An SDR-Based Framework for Cybersecurity Assessment of Vehicle-to-Everything (V2X) Systems," 2024 IEEE International Conference on Cyber Security and Resilience (CSR), London, United Kingdom, 2024, pp. 01-08, doi: 10.1109/CSR61664.2024.10679384.

- Sohail, M.S.; Portomauro, G.; Gaggero, G.B.; Patrone, F.; Marchese, M. Performance Analysis and Security Preservation of DSRC in V2X Networks. Electronics 2025, 14, 3786. https://doi.org/10.3390/electronics14193786

the safety of multiple vehicles simultaneously. To mitigate these challenges open source V2X communications frameworks (OpenC2X, ns-3 with V2X modules, and OpenAirInterface (OAI)) provide reference implementations, enabling transparent validation and controlled penetration testing for control vulnerability assessments.

Beyond these safety oriented domains, infotainment systems connected to V2X networks expand the attack surface. Such systems often integrate with external services including cloud APIs, streaming platforms, Over The Air (OTA) update mechanisms, and mobile applications, creating multiple entry points for attackers [164]. Weaknesses in OTA updates, for example, could be exploited to inject ransomware or malicious firmware, while manipulation of navigation and traffic data could mislead drivers. Similarly, compromised entertainment or media apps may serve as a vector for malware injection. Importantly, once adversaries gain a foothold in the infotainment environment, they may attempt lateral movement into vehicle control systems or V2X communication channels, transforming what appears to be a "non critical" compromise into a severe safety hazard [165].

At the core of these risks are the specialized radio interfaces designed for V2X technologies, namely OBUs integrated into vehicles and RSUs deployed at intersections or along roadways. OBUs typically operate within Vehicular Ad Hoc Networks (VANETs) and support safety critical applications, such as the Alert System for Street Intersections (ASSJ). By leveraging GPS enabled OBUs and RSUs, these systems can detect potential collisions and disseminate warnings to surrounding vehicles in real time [166]. To ensure reliability in such scenarios, vulnerability assessments must simulate realistic attack conditions including manipulated signals, altered timing data, or malicious broadcasts to evaluate how OBUs and RSUs respond under adversarial conditions.

Another important attack vector lies in the On Board Diagnostics (OBD) interfaces, which connect external devices to the vehicle's CAN bus [53]. While OBD interfaces facilitate diagnostics, data collection, and communication between ECUs, infotainment systems, and Transmission Control Units (TCUs) [167], they also open pathways for cyberattacks. Exploiting vulnerabilities in the CAN bus, adversaries can inject falsified messages, issue unauthorized commands, or manipulate sensor data, potentially undermining both safety and vehicle integrity.

Complementing tailored radio interfaces, SDR technology offers a powerful tool for penetration testing within V2X environments [163]. SDR enables the emulation, capture, and manipulation of wireless signals while flexibly adjusting parameters such as frequency, modulation, and bandwidth. This allows testers to conduct detailed packet level analysis and replicate sophisticated attack scenarios using a single hardware platform combined with open source software. By leveraging SDR, stakeholders can systematically evaluate the resilience of OBUs, RSUs, and in vehicle subsystems against both standardized and proprietary communication protocols.

4.1 Regional Security Framework

In the European context, ETSI TS 102 940 [89, 168] defines the trust and privacy management framework for ITS, establishing pseudonymous authentication as the primary mechanism for preserving user privacy. This approach contrasts with the North American Security Credential Management System (SCMS), which emphasizes certificate transparency and controlled linkability to facilitate misbehavior detection

and forensic analysis [169]. ETSI TS 103 097 [88] specifies the security header formats that enable efficient verification of signed messages while minimizing transmission overhead an aspect critical for latency sensitive safety applications.

The European model prioritizes unlinkability of pseudonym certificates to safeguard users against location tracking and profiling. In contrast, the SCMS framework allows correlation of certificates under controlled conditions, thereby supporting accountability and misbehavior detection but at the cost of increased privacy risks [169]. These architectural differences directly influence risk assessment methodologies: privacy-preserving systems may inherently limit the visibility of attack patterns, whereas linkable systems offer stronger misbehavior detection capabilities but create new vectors for privacy concerns.

In parallel, general cybersecurity risk management frameworks, such as NIST SP 800-30 [143] and NIST CSF [144], provide foundational principles for risk analysis, though they require adaptation to the vehicular environment due to its safety critical and real time constraints [130]. Similarly, the ISA/IEC 62443 [145] series, originally developed for industrial control systems, offers transferable methodologies for assessing vulnerabilities in distributed and safety critical infrastructures, and thus holds relevance for V2X security assessment [170]. In conclusion, V2X vulnerability assessment goes beyond the boundaries of traditional IT security evaluation by accounting for the unique interplay between communication integrity, vehicular safety, and real time system performance.

4.2 Related Works: Vulnerability Assessment in V2X Communication

Extensive research and development in V2X communications emphasize the critical importance of vulnerability assessment, particularly in the interaction between OBUs and RSUs. Identifying weaknesses in these communication channels is essential for preemptively mitigating risks that malicious actors could exploit. Since OBUs and RSUs are fundamental to enabling vehicle infrastructure cooperation, securing them is essential for the reliability of V2X systems.

Several works have addressed this challenge from different perspectives. A notable contribution is the cyber kill chain based analysis method in [160], which introduces a formal framework for vulnerability analysis by leveraging insights from real-world car-hacking studies to propose defensive measures. Similarly, Pham et al. [171] highlight a wide range of attack vectors and countermeasures, particularly focusing on scenarios where adversaries gain direct access to in vehicle networks, while El-Rewini et al. [53] provide a systematic classification of threats aligned with Internet Protocol (IP) stack layers. These works collectively underscore the need for multi layered security strategies to mitigate vulnerabilities across V2X interfaces. Table 4.1 links key V2X interfaces and assets to their IP/OSI layers, highlights main attack vectors, and suggests practical mitigation and assessment techniques, such as SDR-based testing, protocol fuzzing, anomaly monitoring, secure OTA updates, and RSU hardening supporting a layered, risk driven approach for securing safety critical V2X deployments.

Table 4.1: V2X System Layers, IP Stack Mapping, Potential Threats, and Mitigation Approaches

V2X Interfaces and Communication Point	**Assets and Communication Interfaces**	**IP Stack Layer**	**Potential Threats**	**Mitigation / Assessment Approach**
Wireless Communication	DSRC, C-V2X (LTE/5G), GNSS	Physical / Data Link	Eavesdropping, spoofing, replay attacks, signal jamming	SDR-based testing, protocol fuzzing, signal integrity verification, cryptographic safeguards
On-Board Units (OBUs)	GPS-enabled units, VANET nodes	Application / Transport	Manipulated signals, altered timing data, false broadcasts, location spoofing	Attack simulations, intrusion detection systems (IDS), anomaly monitoring, secure firmware validation
Roadside Units (RSUs)	Traffic intersections, roadside infrastructure	Network / Data Link	Message injection, unauthorized control commands, physical tampering	SDR penetration tests, packet-level analysis, authentication checks, physical security audits
OBD / CAN Bus	ECU, TCU, infotainment system	Data Link / Application	Message injection, unauthorized commands, sensor manipulation, replay attacks	Secure CAN architecture, message authentication, fuzz testing, anomaly detection
Infotainment / OTA Updates	Cloud APIs, mobile apps, streaming platforms	Application / Transport	Malware injection, ransomware, lateral movement, supply-chain attacks	OTA signature verification, sandboxing, penetration testing, secure update pipelines
Protocols	IEEE 802.11p, 5G-V2X, proprietary protocols	All Layers (varies by protocol)	Protocol exploits, reverse engineering, downgrade attacks	SDR observation tests, simulation-based attack injection, protocol validation, cryptographic enforcement

For instance, authors in [172] develop an SDR-based cybersecurity verification framework for Smart Agricultural Machines (SAMs), where real world cyberattacks on an SDR enabled testbed demonstrated the resilience of proprietary communication protocols. Complementary to this, Pohl et al. [173] present a framework for inferring undocumented wireless protocols, implemented in the open-source tool Universal Radio Hacker [174], advancing security analysis of proprietary systems. These contributions illustrate how SDR technology offers flexible means for vulnerability assessment, enabling detailed packet-level inspection and controlled simulation of attack scenarios [163].

Research has also highlighted the role of diagnostic and internal vehicle communication interfaces in the broader cybersecurity landscape. For example, OBD ports link external devices with the CAN bus, enabling critical functions, such as diagnostics and data exchange, but also exposing vehicles to risks where attackers can manipulate sensor data, inject unauthorized commands, or disrupt vehicle operations [175]. This underlines the need for robust security mechanisms across both external V2X links (OBU–RSU) and internal vehicular networks. In terms of security risk evaluation methodologies, Threat Analysis and Risk Assessment (TARA) approaches have been adapted to vehicular applications. The work in [176] applies TARA to connected car mobile applications, identifying common weaknesses by mapping existing vulnerabilities to security models. Similarly, Ivanov et al. [177] survey cybersecurity challenges in V2X communications and review standardization efforts by ISO, ITU, IEEE, and ETSI, revealing gaps between evolving standards and practical system security. The broader surveys in [178] further emphasize ongoing privacy and security challenges, while also outlining potential defense mechanisms and standardization directions.

Proactive accident prevention applications have also motivated OBU–RSU communication studies. For example, the ASSJ framework [166] integrates GNSS-enabled OBUs with RSUs to calculate potential collision risks and disseminate alerts, demonstrating the safety critical role of reliable V2X communication. However, while such applications illustrate the functional potential of V2X systems, the literature lacks detailed studies addressing vulnerabilities in real-world OBU–RSU communications.

Complementary to system-level and protocol-level assessments, predictive approaches from discrete event system theory provide new perspectives for resilience. Cong et al. [179] address predictability verification of fault patterns in Petri net models, offering computationally efficient methods to detect abnormal system behaviors. Their later work [180] extends this to stochastic discrete event systems with intermittent observation loss, providing conditions for maintaining observability despite missing or corrupted data. Such approaches are directly relevant to V2X systems, where attacks like jamming, spoofing, or replay can cause intermittent loss of CAMs or DENMs.

In summary, the literature demonstrates considerable progress in vulnerability analysis in the automotive, agricultural and general wireless communication domains. Existing research has provided a wide range of tools, including SDR based attack emulation [163, 172], protocol reverse engineering [173, 174], TARA methodologies [176], and predictive fault modeling [179, 180]. Despite these advances, a significant gap remains: although OBU–RSU communication is widely recognized as the backbone of V2X ecosystems, systematic vulnerability assessments of real-world V2X testbeds are still limited. Addressing this gap is crucial for developing secure, resilient, and

trustworthy V2X infrastructures. Addressing the research questions formulated in Chapter 1, this thesis bridges this gap by conducting comprehensive vulnerability assessments that compare industrial V2X systems with lab-based testbeds, thereby evaluating the resilience of V2X communication protocols under realistic operational conditions.

4.3 Security Challenges in V2X

Building upon the comprehensive threat taxonomy and risk management framework established in Chapter 3, this chapter focuses on practical vulnerability assessment methodologies for V2X testbed environments. While Chapter 3 systematically categorizes threats (DoS, jamming, spoofing, replay attacks) and defines risk management principles, this chapter demonstrates their empirical evaluation through controlled experimental platforms. Potential threats include:

- Availability attacks: Jamming and denial-of-service disrupt communication channels.
- Integrity attacks: Message falsification or replay can mislead vehicles, potentially causing accidents.
- Confidentiality breaches: Unauthorized interception of data compromises privacy and operational secrecy.

Among these threats, wireless eavesdropping discussed in Section 3.2 as part of the V2X threat landscape presents unique challenges for testbed-based assessment. Adversaries can covertly capture transmitted signals without detection, gradually building a detailed profile of vehicle activity and network behavior.

Recent studies have demonstrated the feasibility of fine grained application fingerprinting using RF signal analysis. Originally applied to detect Android application activity via energy harvesting, these methods could be adapted to vehicular networks [181, 182]. In the V2X context, attackers may infer sensitive details, such as vehicle trajectories, user routines, or even the status of autonomous control modules. This not only jeopardizes privacy but could also expose vulnerabilities exploitable for coordinated large scale attacks. The mitigation strategies for these threats including cryptographic authentication mechanisms (Section 3.5.1), intrusion detection systems (Section 3.5.2), and privacy preserving certificate schemes are detailed in Chapter 3. This chapter operationalizes these concepts through SDR-based testbed implementations that enable empirical measurement of attack effectiveness and defense resilience.

4.4 Reference Architecture and Testbed Design

Systematic vulnerability assessment requires controlled experimental environments that accurately replicate real world V2X communication scenarios. This section presents two complementary testbed architectures developed for security evaluation: an SDR-based emulation platform (developed in SCNL lab at University of Genoa) providing protocol level flexibility, and an industrial grade commercial Cohda Wireless

equipment(acquired from Cohda Wireless) representing deployed V2X infrastructure. These dual testbeds enable comparative analysis of vulnerabilities across both research and production implementations, thereby validating the generalizability of identified security weaknesses.

To empirically evaluate the security of DSRC-based V2X communications, a flexible and software defined emulation testbed was developed. The core of this testbed is built upon GNU Radio Companion (GRC) [183], an open-source software development toolkit that facilitates signal processing and SDR control. The flowgraphs for this research were developed using the open source libraries gr-foo and gr-ieee802-11 for GNU Radio. These libraries provide essential, pre-built signal processing blocks for frame detection, synchronization, equalization, and decoding that are specifically designed for the IEEE 802.11 family of standards, including the 802.11p variant [184]. This platform allows for the precise emulation of an IEEE 802.11p-based OBU and RSU, forming the foundation for our security assessment experiments. The following subsections detail the implementation of the receiver (OBU) and transmitter (RSU) flowgraphs.
[2]

4.4.1 Tier 1: SDR-Based Emulation Testbed

The SDR-based emulation testbed was designed and implemented by the author in SCNL Lab at University of Genoa, using commercially available hardware components (Ettus USRP B210, Nuand BladeRF) and open-source software frameworks (GNU Radio Companion, gr-ieee802-11, gr-foo libraries). The author's original contributions include:

- Integration architecture design for dual SDR attack monitor configuration.
- Systematic attack scenario methodology categorizing attacks by complexity.
- Custom GNU Radio flowgraph implementation for 802.11p packet generation and attack emulation.
- Experimental evaluation protocol with performance metrics.
- Cross protocol vulnerability discovery validated against commercial equipment [21, 185].

OBU Receiver Implementation

The receiver flowgraph *wifi_rx_OBU.grc* (Figure 4.1) contains frame detection, synchronization, and decoding blocks for IEEE 802.11p packet reception. It demodulates and decodes incoming IEEE 802.11p packets from the wireless channel. Leveraging the gr-ieee802-11 library, it ensures the implementation of a standard compliant physical layer, which is critical for the validity of the security assessments. The design of the receiver is modular, separating the tasks of signal acquisition, synchronization,

[2]
- https://github.com/bastibl/gr-foo
- https://github.com/bastibl/gr-ieee802-11

and data extraction. The flowgraph is strategically structured into two main functional sections: an upper section dedicated to frame detection and synchronization, and a lower section focused on frame decoding and data interpretation.

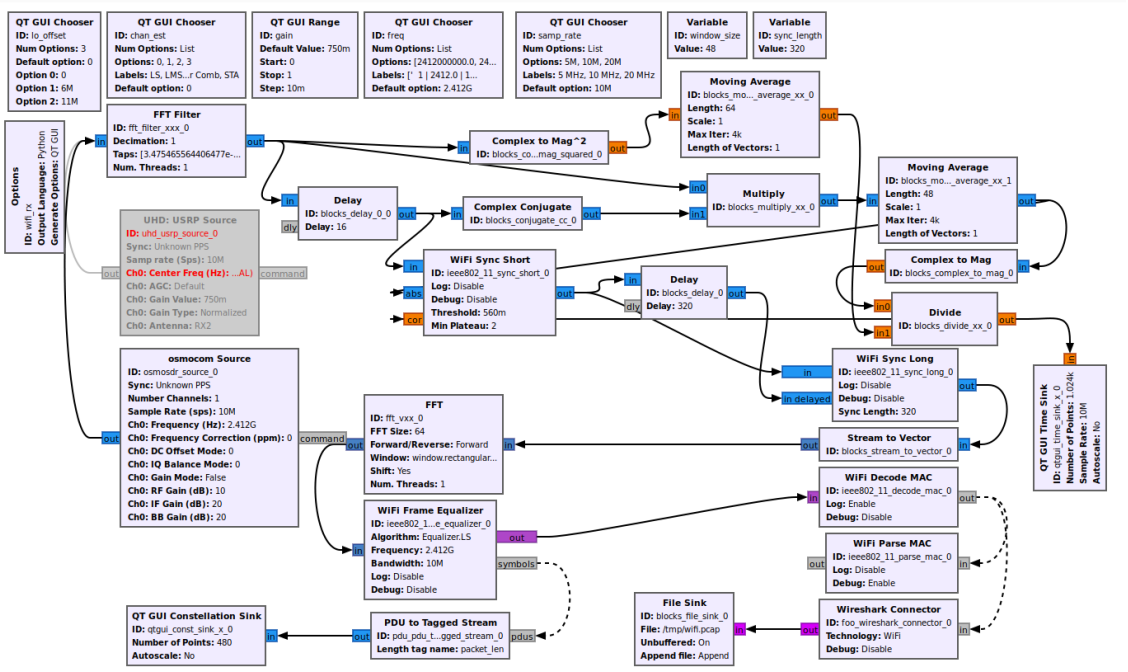


Figure 4.1: GNU Radio flowgraph implementation of OBU

The signal processing chain begins with the Osmocom Source block (or alternatively, a UHD: USRP Source block when using Ettus hardware), which serves as the interface to the SDR hardware. This block is configured to capture signals at a center frequency of 5.89 GHz, precisely aligned with the European ITS band for DSRC communications, and a sample rate sufficient to cover the standard's 10 MHz bandwidth. The incoming signal is then fed into the two parallel processing paths:

- Upper Section - Frame Detection and Synchronization: This path is critical for robust operation in the challenging vehicular environment. It is responsible for ensuring that incoming signals are properly identified and synchronized. The core of this functionality lies in the WiFi Sync Short and WiFi Sync Long blocks. These blocks play a critical role by detecting the specific preamble sequences defined in the IEEE 802.11p standard. The WiFi Sync Short block performs an initial, coarse detection to identify the presence of a packet and correct for major time and frequency offsets. Subsequently, the WiFi Sync Long block provides fine-grained synchronization, allowing the receiver to accurately lock onto the start of the OFDM symbols within the frame. This two-stage process is essential for compensating for the Doppler shifts and timing inaccuracies common in high-speed scenarios.

- Lower Section - Frame Decoding and Data Extraction: Once a frame is detected and synchronized, the signal proceeds down the lower path for decoding. This section focuses on interpreting the captured signal into meaningful data. The synchronized signal first passes through a Stream to Vector block to prepare it for the FFT operation, which converts the time-domain OFDM signal

into its frequency-domain subcarriers. The WiFi Frame Equalizer block then compensates for channel distortions, such as multi-path fading, using the information from the preamble. The equalized subcarriers are then passed to the WiFi Decode MAC block, which demodulates the symbols (e.g., using BPSK/QPSK) and performs de-interleaving and Forward Error Correction (FEC) decoding to recover the original bitstream. Finally, the WiFi Parse MAC block interprets this bitstream to precisely reconstruct the IEEE 802.11p MAC frame from the air interface, extracting the MAC header and payload.

The output of the decoding chain is versatile, facilitating comprehensive analysis. The decoded data can be stored in a binary file for post-processing using a File Sink block. More critically for real-time assessment, the data is forwarded directly to the Wireshark network protocol analyzer via a Wireshark Connector block [186]. This enables real-time packet analysis, allowing the experimenter to inspect the content of CAMs or DENMs as they are received.

This modular design is a key strength of the SDR-based setup, as it facilitates flexible adaptation to various experimental conditions, including tests involving signal interference or packet manipulation. The parameters for each block, such as channel selection (frequency), receiver gain, and sample rate, can be dynamically adjusted through QT GUI controls, enabling quick reconfiguration for different test scenarios without modifying the underlying code. This flexibility is fundamental for conducting reproducible security assessments under a wide range of conditions.

RSU Transmitter Implementation

The complementary transmitter flowgraph `wifi_tx_RSU.grc` (Figure 4.2) at RSU contains packet generation, MAC/PHY layer processing, and RF transmission blocks for IEEE 802.11p. It generates and transmitting standard compliant IEEE 802.11p packets. Its design mirrors the layered structure of the protocol stack, moving from data generation to physical layer modulation. Like the receiver implementation, this flowgraph leverages the open-source gr-ieee802-11 library to ensure full compliance with the IEEE 802.11p standard, enabling interoperability with other standard-compliant devices.

The transmission chain operates as follows, implementing a complete transmit pipeline from application data to RF transmission:

- Packet Generation and Interface: The flowgraph begins with a Message Strobe block that generates periodic data packets containing a predefined payload. The transmission interval is configurable, with a typical setting of 300 ms to simulate the periodic broadcast of CAMs by infrastructure units [13]. For more dynamic testing scenarios requiring custom message content, a Socket PDU block is incorporated, which accepts packets from external applications via a TCP server socket on port 52001. This network interfacing capability allows for real time injection of various message types, including DENM [14] and SPaT messages [11].

- Signal Conditioning and Frame Preparation: Following packet generation, the signal undergoes several conditioning steps. The Multiply Constant block scales the signal amplitude to appropriate levels, while the Packet Pad2 block ensures

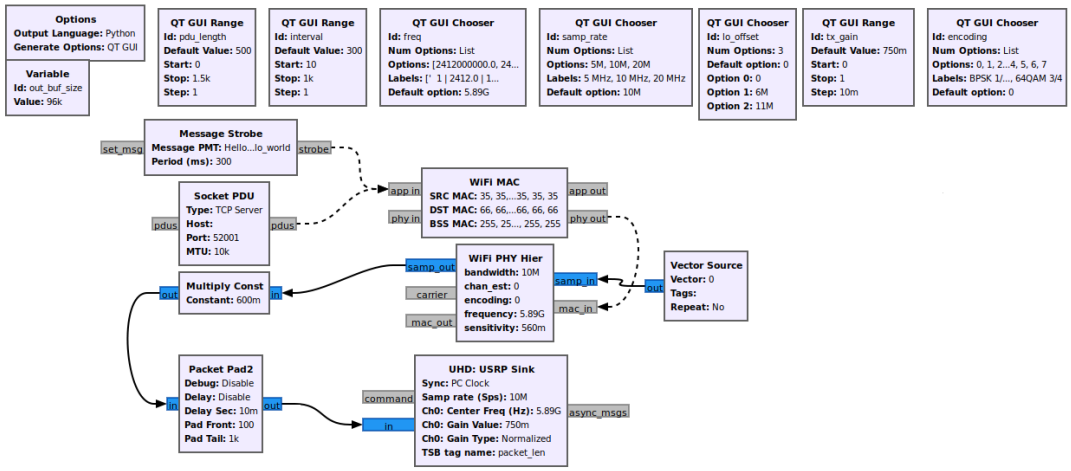


Figure 4.2: GNU Radio flow graph implementation of the RSU

proper packet alignment and formatting. This preparation stage is crucial for maintaining signal integrity throughout the transmission chain.

- MAC and PHY Layer Processing: The conditioned signal then passes through the core communication blocks. The WiFi MAC block encapsulates the application data into a valid IEEE 802.11 MAC frame [187], adding necessary header fields including source and destination MAC addresses (configured as 35:35:... and 66:66:... respectively for this emulation). The WiFi PHY Hier (Physical Layer Hierarchical) block implements the specific physical layer parameters of the IEEE 802.11p standard, configured for operation at 5.89 GHz center frequency with 10 MHz bandwidth, compliant with the DSRC protocol. This block performs several essential functions:
  - Scrambling: Randomizes data bits to prevent long sequences of 1s or 0s.
  - FEC Encoding: Adds redundancy for error correction.
  - Interleaving: Rearranges bit order to mitigate burst errors.
  - OFDM Modulation: Maps encoded bits to subcarriers using configurable modulation schemes (BPSK, QPSK, etc.) [4] and generates time-domain OFDM symbols with preamble sequences.
- RF Transmission and Parameter Control: The processed signal is finally transmitted via the UHD: USRP Sink block, which interfaces with the SDR hardware to convert digital samples to analog RF signals at the specified 5.89 GHz center frequency. The SDR-based setup allows dynamic adjustment of key communication parameters including channel selection, transmission power, modulation schemes, and coding rates through QT GUI controls. This flexibility enables rapid reconfiguration for different experimental scenarios without modifying the underlying flowgraph structure.

The complete GNU Radio Companion flowgraphs *wifi_rx_RSU.grc* and *wifi_tx_RSU.grc* are available in the GitHub repository, providing full transparency and reproducibility for the transmission system. This transmitter implementation, combined with the receiver flowgraph, establishes a complete SDR-based emulation platform capable of generating legitimate V2X traffic while providing the foundation for developing and testing sophisticated cyber attacks through modification of these core flowgraphs, as detailed in subsequent sections.

4.4.2 Tier 2: Industrial V2X Equipment Testbed

The industrial grade testbed leverages commercial Cohda Wireless MK6C equipment featuring dual V2X technology (DSRC and C-V2X). The author's contribution lies in developing a systematic vulnerability assessment framework that evaluates commercial V2X devices against realistic attack scenarios using SDR-based emulation. This methodology ensures research findings are validated against industrial standards and real-world deployments.

The Industrial Testbed (Cohda Wireless: Commercial-Grade Implementation)

To validate the proposed security assessment framework against industrial-grade systems and specifically evaluate the vulnerability of V2X communications at both the protocol and implementation levels, and the risks associated with these vulnerabilities, a commercial testbed was acquired using standard V2X equipment. The Industrial V2X testbed employs MK6 Cohda Wireless OBU and RSU devices as shown in Figure 4.3, representing the state-of-the-art technology currently deployed in real-world intelligent transportation systems. This commercial setup was intentionally selected to conduct comparative vulnerability analysis, examining how real-world implementations withstand attacks that exploit weaknesses in both the underlying IEEE 802.11p protocol and the higher-layer security mechanisms.

4.4.3 Hardware Architecture and Capabilities

The industrial testbed, illustrated in Figure 4.3, comprises complementary MK6 OBU and RSU units that form a complete V2X communication ecosystem. These sixth-generation devices represent a significant advancement in vehicular communication technology, featuring dual-mode V2X capability with both DSRC and C-V2X support.

The hardware architecture is composed of the following components and equipped with the following communication interfaces:

- Processing Unit: An i.MX8 application processor delivering 8544 DMIPS computational power;
- DSRC Communication: Dual NXP RoadLink SAF5400 chipsets providing robust DSRC capability;
- Cellular V2X: Qualcomm SA515 chipset supporting 3GPP R15 and 5G standards;
- Connectivity Suite: Comprehensive interfaces including:

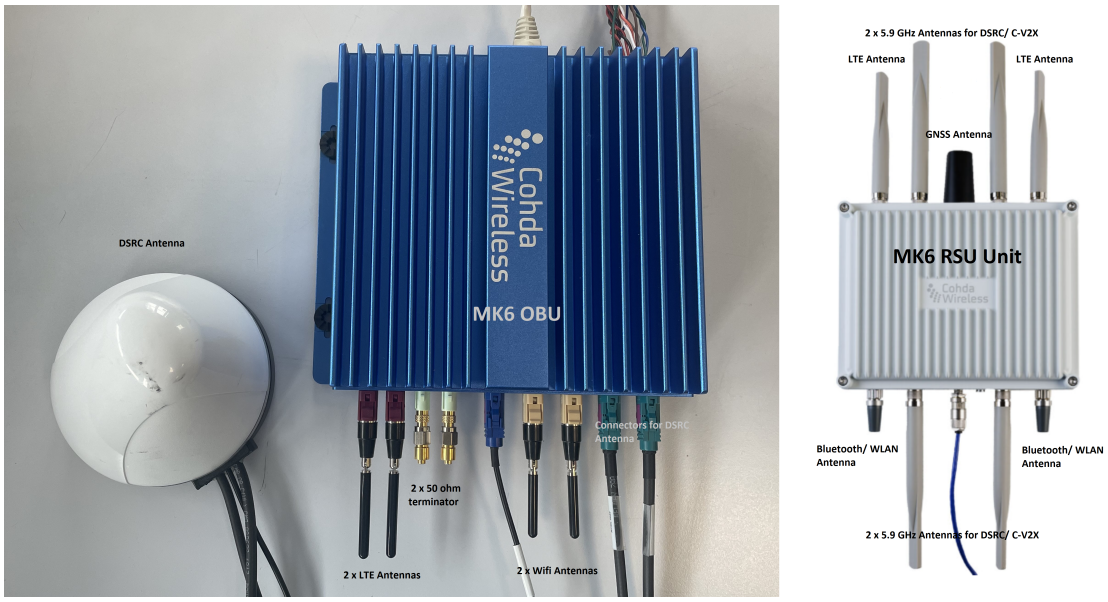


Figure 4.3: MK6 Cohda Wireless OBU and RSU Testbed for Industrial V2X Communication Systems.

- Cellular 5G NR with 4G/3G/2G fallback capabilities
- Wi-Fi (802.11a/b/g/n/ac) dual-band 2.4/5 GHz
- Bluetooth connectivity
- Ethernet (10/100/1000BASE-T)
- CAN-FD (up to 5Mbps) for vehicle bus integration
- Automotive Ethernet (100BASE-T1)
- GNSS receiver (U-Blox M9N) for precise positioning

This robust hardware foundation ensures reliable operation in demanding automotive environments while providing multiple communication pathways for redundant safety critical applications. The acquisition of this commercial system enables direct testing of how industrial implementations handle protocol-level vulnerabilities inherent in the IEEE 802.11p standard.

4.4.4 Synchronization, Timing, and Location

Accurate synchronization of time and position is fundamental to both KPI computation and security validation within V2X systems. On the ITS-G5/WAVE bearer, multi-channel operation follows the coordinated interval model defined in IEEE 1609.4 [12], in which each 100 ms synchronization interval is partitioned into nominal 50 ms CCH and Service Channel (SCH) windows. Slot alignment is maintained through the WAVE Timing Advertisement (WAVE TA) mechanism, while Outside the Context of a BSS (OCB) access behavior and MAC timing primitives are specified by IEEE 802.11-2016 [187].

Location and timing sources for stations rely on GNSS receivers coupled with 1PPS-disciplined oscillators, ensuring UTC-aligned timestamps across all components [13]. Core V2X message types, namely CAMs and DENMs [76] carry essential

mobility information such as position, speed, heading, and associated confidence levels, thereby supporting mobility aware analysis and cross validation.

Security mechanisms additionally depend on temporal consistency. Message freshness is derived from generation times and validity intervals encoded in IEEE 1609.2 [61] and ETSI TS 103 097 [78] security headers. Verification processes compare these fields against the station's UTC reference, with acceptance and rejection causes logged for subsequent audit and forensic analysis.

For performance monitoring, all logging entities (both SDR-based loggers and software protocol stacks) must produce monotonic, UTC-referenced timestamps for frames and Facilities-layer PDUs. This ensures reproducibility of metrics such as latency, Packet Delivery Ratio (PDR) as a function of distance, and CBR. CBR observation windows and congestion control state transitions are implemented according to ETSI DCC [76].

4.4.5 Software Framework and Development Environment

The industrial testbed operates using the MKx SDK, an Integrated Development Environment built on Ubuntu 20.04 Linux and designed to run within virtual machine environments (VMware or Oracle VirtualBox). The SDK provides a comprehensive software stack for V2X application development [2], including the ETSI-compliant application examples that demonstrate practical implementation of V2V and V2I communications. The software architecture leverages the V2X Lib Network and Facilities Layers, enabling developers to utilize Cohda Wireless Stack APIs for creating sophisticated V2X applications. To evaluate V2X communication in the industrial test bed, the specific operational behaviors of the OBU and RSU are outlined below:

- OBU Operations: Transmission of CAMs [13] containing critical vehicle data including position, speed, heading, and acceleration.

- RSU Operations: Broadcasting of DENMs [14] for hazard warnings, MAP/SPaT messages for traffic signal information, and In-Vehicle Information (IVI) for driver advisories.

This software environment allows for precise vulnerability testing by enabling controlled manipulation of message parameters to assess the robustness of the security implementations against protocol-level exploits.

The key experimental parameters for both testbeds are summarized in Table 4.2.

Table 4.2: Experimental parameters for security assessment tests.

Parameter	**Emulation Testbed**	**Industrial Testbed**
Center Frequency	5.89 GHz	5.89 GHz
Bandwidth	10 MHz	10 MHz
Sample Rate	20 Msps	N/A (Commercial)
TX Gain (OBU)	30 dB	Auto-controlled
RX Gain (RSU)	40 dB	Auto-controlled
Antenna Type	Omnidirectional	Integrated
Distance (OBU-RSU)	5–50 m	5–50 m
Packet Rate (CAM)	10 Hz	10 Hz
Jammer EIRP	20 dBm	20 dBm
SNR (Normal Operation)	15–20 dB	20–25 dB
INR (During Jamming)	−10 to −5 dB	−5 to 0 dB

The reference architecture presented in Section 4.4 incorporates a wireless communication segment with its distinctive characteristics. In the V2X domain, this architecture underpins the exchange of safety critical information between OBUs and RSUs using protocols such as IEEE 802.11p/DSRC and C-V2X. While these protocols are designed to ensure low-latency and reliable message delivery, the open and broadcast nature of V2X communication increases the potential attack surface. Unlike isolated OT systems that may benefit from air-gapped designs, V2X systems operate in highly dynamic environments where malicious interference, spoofing, or message manipulation can directly threaten both vehicular safety and traffic management. The vulnerability assessment of V2X protocols operationalizes the security attributes (availability, integrity, confidentiality) and temporal constraints defined in Section 3.2. Specifically, this testbed-based evaluation measures how protocol implementations withstand attacks (message injection, replay, spoofing, jamming) under controlled conditions, providing empirical validation of the risk scenarios catalogued in Chapter 3.

4.5 Potential V2X Attack Scenarios within the Systematic Vulnerability Assessment Framework

The heterogeneity of V2X communication technologies requires a structured and progressive methodology for vulnerability assessment. This section presents a systematic framework that evaluates increasingly sophisticated potential attack scenarios, ranging from physical-layer interference to multi-vector cyber exploits. The objective is to assess protocol resilience at each stage and classify risks according to their impact on safety-critical vehicular functions, consistent with the risk assessment methodology introduced in Chapter 3. Figure 4.4 illustrates the decision tree structure guiding this evaluation process.

A comprehensive assessment begins with the collection of low-level radio and protocol parameters, including operating frequency band (e.g., 5.9 GHz ITS-G5/DSRC), channelization, transmission power, bandwidth, MAC behavior, and duplexing characteristics. These parameters may be obtained from OBU/RSU specifications or

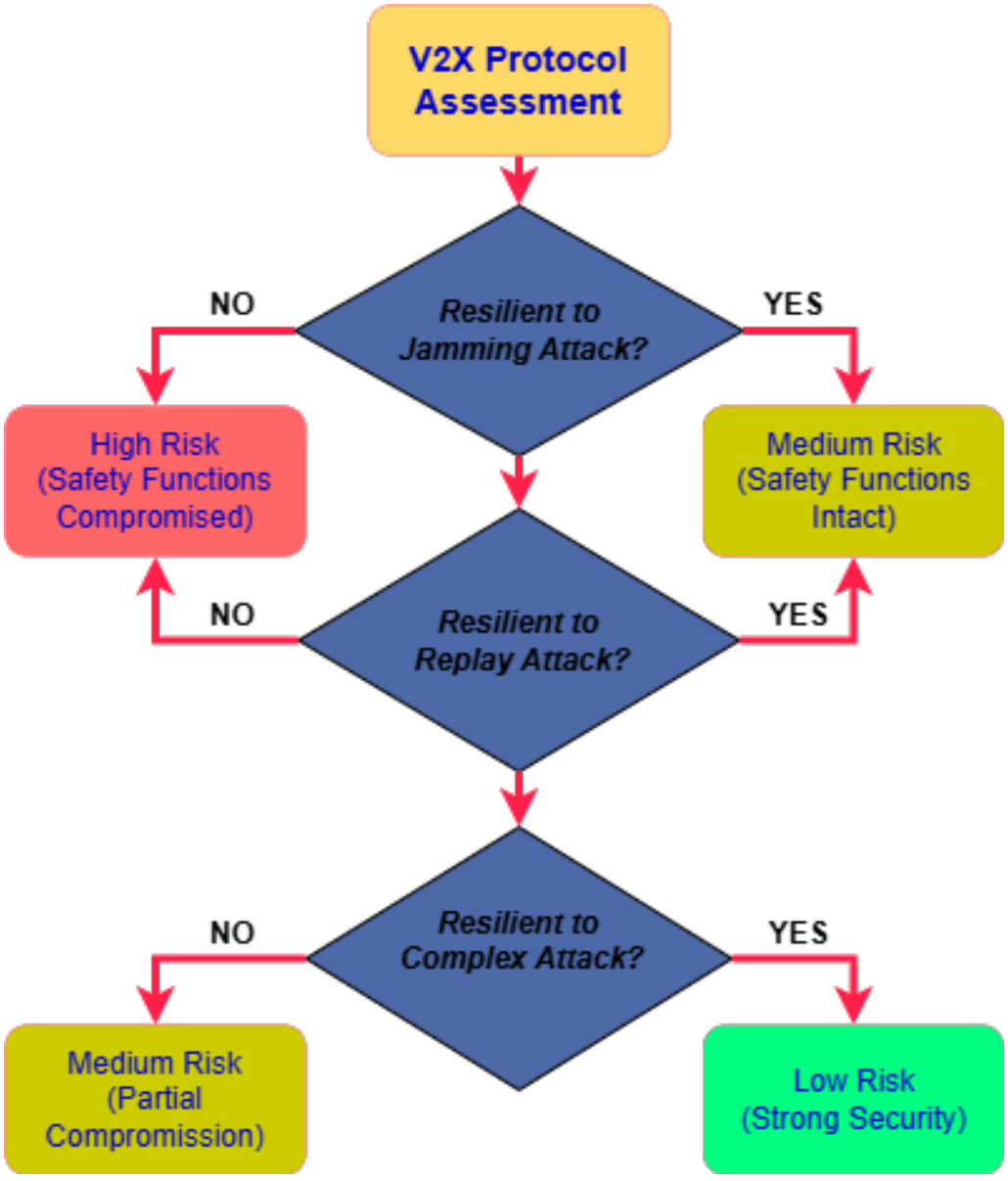


Figure 4.4: Flow chart(decision tree) of the vulnerability assessment framework proposed.

empirically measured using SDR platforms and spectrum analysis tools. This baseline characterization enables controlled testing of protocol robustness under adversarial conditions. The framework evaluates six categories of potential V2X attacks, ordered by increasing sophistication:

- Denial of Service (DoS) via jamming: deliberate interference aimed at denying or degrading V2X message delivery (affecting CAMs, DENMs, MAP/SPaT, etc.) [188].
- Replay attacks: retransmission of previously captured legitimate V2X messages to induce erroneous behavior [171].
- Reverse engineering: analysis of protocol formats and device behavior to craft valid, malicious V2X messages without relying on captured traffic [173].
- Spoofing attacks: an adversary deliberately sends false information into the network while pretending to be a legitimate vehicle or infrastructure node [3]. This can result in the creation of "phantom" vehicles that do not actually exist, or false traffic conditions such as congestion or accidents. Such attacks can mislead other vehicles and traffic management systems, causing unsafe driving decisions, traffic jams, or inefficient route planning.
- Sybil attacks: A Sybil attack [177] occurs when a single malicious entity generates multiple fake identities within the network. By controlling these identities, the attacker can manipulate system-wide decisions, influence consensus mechanisms, or overwhelm data aggregation processes. In vehicular networks, this can lead to false traffic information, erroneous cooperative driving decisions, or disruption of network trust mechanisms, since the system assumes each identity represents an independent, legitimate vehicle.
- Complex attacks: combinations of the above techniques (e.g., selective jamming combined with forged messages) to obtain finer, more damaging control over vehicular or infrastructure behavior.

The framework evaluates the resilience of IEEE 802.11p-based V2X protocols against cyberattacks, ultimately classifying risk levels as low, medium, or high, depending on whether critical safety functions (collision avoidance, hazard warnings, or cooperative driving support) are compromised.

- Jamming Attack Assessment

  The first step is to test whether the V2X channel is resilient to jamming. Jamming in V2X can prevent the transmission of critical safety messages, such as CAMs or DENMs. If resilience is lacking, the next step is to assess whether the disruption of communication directly compromises critical safety functions.

  - If safety critical functions (e.g., collision warnings) fail, the system is classified as high risk.
  - If safety functions remain operational through redundancy (e.g., fallback to sensors or C-V2X), the system is classified as medium risk.

Some advanced forms of jamming include reactive jamming [189], in which the jammer adapts to channel switching or detects active transmissions to selectively block packets in real time, and protocol-aware jamming, in which truncated or forged ITS-G5 frames are transmitted to exploit receiver processing and more effectively disrupt legitimate traffic.

- Replay Attack Assessment

  If the system demonstrates resilience to jamming, the next step is to assess replay attacks. In V2X, attackers may replay recorded CAMs to create ghost vehicles or resend old DENMs to generate false hazard warnings. Depending on authentication and timestamp verification:

  - If replay compromises vehicle safety or traffic flow, the risk is high.
  - If the replayed messages are detected and ignored due to security checks (e.g., timestamp freshness or pseudonym validation), the risk is low.

  Replay attacks can take several forms for example, Simple Replay, where raw V2X frames are captured and resent without modification and Interaction-Aware Replay, where attackers account for session-based exchanges such as pseudonym certificate validation or acknowledgment protocols, but the worst ones are Ghost Vehicle Injection, where replayed CAMs trick nearby vehicles into reacting to non-existent entities.

- Reverse Engineering Assessment

  If the system withstands jamming and replay attempts, it is evaluated against reverse engineering. Here, attackers attempt to understand the encoding of V2X messages (e.g., ASN.1 PER encoding of CAMs/DENMs) or security certificates to craft malicious payloads.

  - If reverse engineering does not compromise core safety functions due to robust cryptographic protections, the system is low risk.
  - If it enables adversaries to craft valid looking but malicious V2X messages, the system is medium risk.

- Complex Attack Scenarios

  Complex attacks combine methods for greater impact. For instance:

  - Selective Jamming + Replay: selectively blocking certain DENMs while replaying outdated hazard alerts to cause accidents.
  - Rogue RSU Deployment: replacing a legitimate RSU with a malicious one that injects fake MAP/SPaT messages, misleading vehicles about traffic signal states.
  - Controller Takeover: blocking legitimate OBU transmissions while injecting crafted CAMs from a rogue OBU, effectively hijacking cooperative awareness.

These scenarios demonstrate how attackers leveraging multiple techniques can undermine V2X safety services, especially in the absence of strong authentication, integrity verification, and anomaly detection mechanisms.

Each of these attack types will be elaborated upon in the following sections, with a detailed explanation of the attack implementation provided Risk Levels in V2X Protocol Assessment:

- High Risk: safety critical functions (e.g., collision avoidance, hazard notification) are compromised due to the system's inability to resist a specific attack.
- Medium Risk: System resilience is lacking for some attacks, but redundancy or detection mechanisms prevent full compromise of safety functions.
- Low Risk: The protocol demonstrates resilience across all tested attacks (jamming, replay, reverse engineering), ensuring reliable safety message delivery.

This stepwise framework ensures a structured evaluation of V2X communication protocols, balancing resilience to cyberattacks with the preservation of safety critical vehicular functions.

Each step in the evaluation framework systematically tests the resilience of the the V2X wireless protocol under evaluation against progressively sophisticated cyberattacks. Following the methodology outlined in the previous section on risk in V2X protocols, if the protocol demonstrates sufficient resilience, the assessment advances to the next security level. Conversely, if vulnerabilities are detected, the focus shifts to determining whether these weaknesses impact the critical functions of the V2X system, such as safety critical message delivery, vehicle coordination, or emergency response communications. Based on this analysis, a risk classification is assigned: low risk indicates that the protocol maintains robust security and operational continuity, whereas high risk highlights significant vulnerabilities that could compromise critical V2X operations.

4.6 Framework implementation architecture

4.6.1 SDR-Based Security Assessment Tool

The primary technology used in the design of our security assessment tool is Software-Defined Radio (SDR) [163]. The design of an SDR system integrates flexible hardware and reconfigurable software to enable real-time signal processing across multiple communication standards. The hardware front-end (e.g., USRP, LimeSDR, or RTL-SDR) captures and transmits radio signals, while device drivers (UHD, SoapySDR, or rtl-sdr) provide the interface between hardware and software. GRC is employed to design block diagrams that represent the digital signal processing chain, including modulation, filtering, and decoding. Owing to its open source nature, SDR enables rapid prototyping, protocol testing, and experimentation with custom waveforms, making it a powerful tool for both research and practical wireless communication development [183]. By employing SDR cards, the tool is developed as a flexible and modular solution that can be easily reconfigured and applied to different communication protocols, including V2X. The overall structure of the tool, along with its essential hardware and software elements, is illustrated in Figure 4.5. It supports

both passive monitoring and active attack execution, making it possible to carry out a thorough security evaluation of V2X communication systems under controlled laboratory conditions.

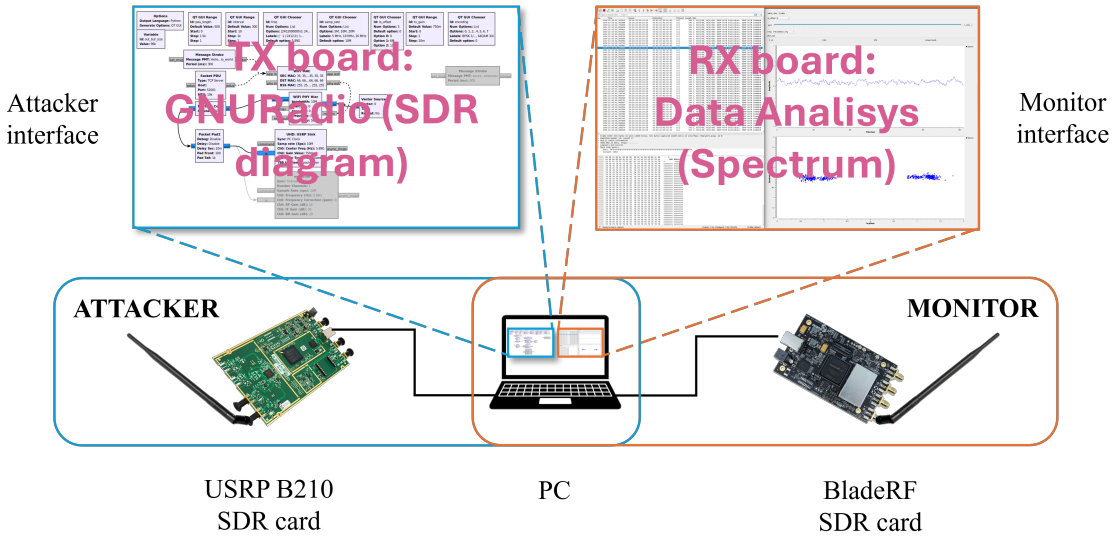


Figure 4.5: SDR-based security assessment tool: System architecture showing dual SDR configuration for simultaneous attack generation and monitoring.

Two SDR cards are connected a PC, allowing the tool to carry out security tests while simultaneously observing their outcomes. The tool comprises two components: (i) Attacker, which uses an Ettus USRP B210 SDR card to perform various cyber attacks, such as jamming and replay attacks, on chosen wireless channels; (ii) Monitor, which uses a BladeRF SDR card to observe the attacked channels passively, intercept data, and evaluate the effectiveness of the attacks.

The Attacker is implemented in GRC configuring the SDR card by programming the appropriate signal processing flow graphs to realize the selected attacks. The Monitor uses GRC to receive signals and Wireshark to display packet structures captured over the monitored channel. The GNU Radio flow graphs were implemented using the open-source gr-foo and gr-ieee802-11 libraries. These libraries provide built blocks for frame detection, frame decoding, and packet transmission tailored to the IEEE 802.11p standard [150, 184]. Together, these tools enable a detailed inspection of data flows, frame structures, and modulation schemes.

To validate our proposed security assessment tool, we consider a reference scenario with a single V2I link between a vehicle equipped with a DSRC OBU, capable of transmitting and receiving IEEE 802.11p packets, and a DSRC RSU, representing a node of the terrestrial infrastructure capable of exchanging data with the vehicle. We implemented this reference scenario in two different ways, building two different testbeds, whose system architectures are shown in Figure 4.6. In the first testbed, called Emulation V2X testbed, two PCs with an SDR card each are configured to transmit and receive IEEE 802.11p packets, operating as OBU and RSU, respectively, as shown in Figure 4.6, left side.

Figure 4.7 depicts the Monitor interface of the proposed emulation testbed (left side of Figure 4.6), showing the packet list, time domain waveform, and constellation diagram of the signals captured from the selected channel. Similar monitoring results were obtained from the industrial testbed (Cohda Wireless), illustrated on the right

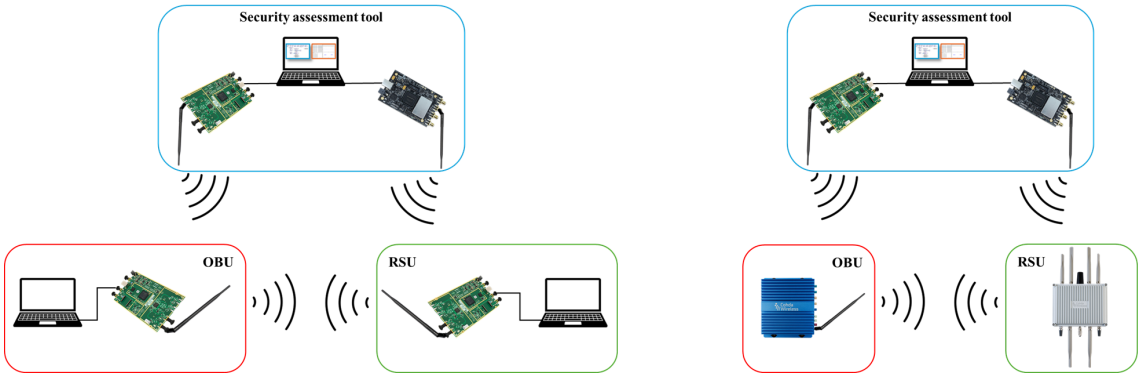


Figure 4.6: System architectures of the implemented emulation testbed (**left**) and industrial testbed (**right**) for V2X communications.

side of Figure 4.6. The constellation diagram reveals a dense clustering of points around the origin with limited dispersion, which is characteristic of a low-order digital modulation scheme such as BPSK, widely employed in the IEEE 802.11p physical layer. The proximity of the observed points to their ideal constellation positions indicates that the signal maintains a relatively high SNR, although minor deviations and spreading suggest the presence of slight noise or distortion effects.

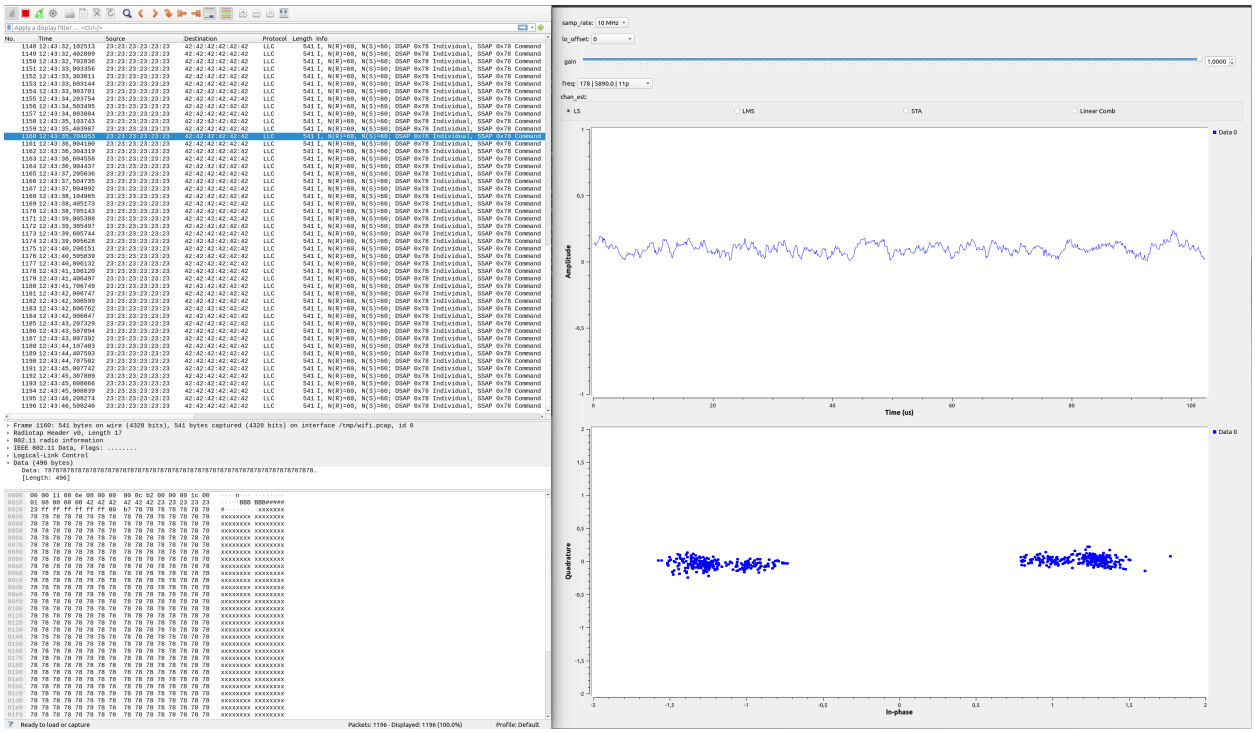


Figure 4.7: SDR-based security assessment tool: Monitor interface showing received packet list (**left**) and signal analysis with time domain representation and BPSK constellation plot (**right**) during normal IEEE 802.11p packet transmissions.

4.6.2 Reproducibility and Open Source Implementation

To ensure full reproducibility of our research findings, we provide comprehensive details about our experimental setup and software implementation. The complete

GRC flowgraphs for all essential components are available in a public repository. The repository includes the following:
[3]

- Core GNU Radio flowgraph files: `wifi_tx_RSU.grc` (RSU transmitter), `wifi_rx_OBU.grc` (OBU receiver), `jamming_attack.grc` (jamming implementation), `capture_for_replayattack.grc` and `transmitter_replay.grc` (replay attack phases), and `transmitter_108.11p_cohdawireless_replayattack.grc` (Cohda Wireless compatibility);
- Environment setup script (`setup_env.sh`) for GNU Radio 3.8.5 configuration;
- Hardware requirements and system configuration details (`checklist.txt`);
- Detailed receiver operation instructions (`INSTRUCTION_RX.txt`).

Our implementation utilizes specific library versions to ensure compatibility and reproducibility: gr-foo and gr-ieee802-11 libraries from github.com/bastibl, GNU Radio Companion v3.8.5.0-6-g57bd109d, and Python 3.8.10. The system was tested on Ubuntu 20.04.6 LTS with the specific hardware configuration described in the repository's hardware requirements document. The experimental setup requires three USRP B210 SDR units, one BladeRF units, and four dedicated Ubuntu systems as detailed in the provided checklist. The Data Availability Statement has been updated to reflect the public availability of these essential reproducibility resources.

4.6.3 Selected Attack Scenarios for Framework Validation

To evaluate the robustness of the proposed vulnerability assessment framework, a selected set of representative attack scenarios is considered. Specifically, the validation focuses on three categories: (i) assessment of the framework implementation architecture under adversarial conditions (Denial of Service through Jamming), (ii) replay attacks targeting message freshness and authentication mechanisms, and (iii) complex attacks formed by combining two techniques to evaluate layered defense resilience. These attack scenarios are used to systematically test the architectural design and its ability to preserve safety-critical V2X functionality.

4.6.4 Denial of Service through Jamming

The most common type of DoS attack in wireless communications is jamming. The considered jamming attack is based on generating Gaussian noise with high amplitude to overwhelm the communication channel by simulating strong environmental interference within the target 5.9 GHz frequency band. The mathematical model for the jamming attack can be expressed as follows:

$$P_{jam}(t) = A \cdot n(t) \cdot \cos(2\pi f_c t + \phi(t)) \tag{4.1}$$

where $P_{jam}(t)$ is the jamming signal power at time t, A is the amplitude scaling factor, $n(t)$ is the Gaussian noise component with zero mean and variance σ^2, f_c is the center frequency (5.896 GHz), and $\phi(t)$ represents the phase modulation component.

[3]The project's source code and related materials are available in the associated GitHub repository.: https://github.com/saadsohail1987-hue/V2X-DSRC-Security-Assessment

The Signal-to-Interference-plus-Noise Ratio (SINR) at the receiver is given by:

$$SINR = \frac{P_s}{P_{jam} + P_n} \tag{4.2}$$

where P_s is the legitimate signal power, P_{jam} is the jamming power, and P_n is the background noise power. Successful jamming occurs when $SINR < \gamma_{threshold}$, where $\gamma_{threshold}$ is the minimum SINR required for successful packet decoding. Figure 4.8 shows the GNU Radio Companion flow graph (`jamming_attack.grc`) developed to implement the considered jammer. It is made up of functional blocks that are in charge of noise generation, signal modulation, amplification, and transmission over a specific frequency band. In detail, a high-amplitude Gaussian noise source is at the core of the jammer (*Noise Source* block) and a cosine waveform is used to introduce modulated interference (*Signal Source* block). By modulating this waveform (*Frequency Mod* and *Phase Mod* blocks), the jammer is able to effectively target and disrupt systems to create a versatile attack vector against different wireless communication protocols. To ensure effective jamming, the signals generated by both the noise source and the modulated signal are amplified by using the *Multiply Const* block, which ensures that the jamming signal power is sufficient to dominate legitimate signals in the target frequency band. The jammer signal is refined by using a *Low Pass Filter* block. The low-pass filter is configured with a decimation factor of 1 and a cutoff frequency of 12 MHz, with a transition width of 1k by using a Hamming window. The filter ensures that the transmitted signal remains within the desired bandwidth, focusing the interference on the targeted frequencies while minimizing unnecessary disruption to neighboring channels. The amplified and filtered interference signal is transmitted by the USRP B210 SDR card by using the *osmocom Sink* block and setting the center frequency of the jammer at 5.896 GHz. The *Selector Block* is another crucial component of the jammer design because it enables the operator to switch between multiple input signals, such as different modulated waveforms or noise sources, allowing rapid implementations of different jamming techniques. This flexibility is particularly useful in multi-protocol environments, where the jammer may need to switch between targeting systems by using different modulation schemes or frequencies. The *QT GUI* blocks allow monitoring the target channel. The *QT GUI Frequency Sink*, *QT GUI Waterfall Sink*, and *QT GUI Time Sink* blocks provide real-time visualization of the frequency spectrum, power distribution over time, and time domain representation of the transmitted signal, respectively.

4.6.5 Replay attack

A replay attack is an attempt to send malicious commands from a fake controller by retransmitting previously captured signals. Replay attacks can exploit vulnerabilities in V2X communication systems by exploiting the lack of robust message authentication and verification processes. The mathematical model for a replay attack can be described as follows:

Let $M(t_0)$ be a legitimate message transmitted at time t_0. The replay attack involves capturing and retransmitting this message at time $t_1 > t_0$. The replayed message $M'(t_1)$ can be expressed as:

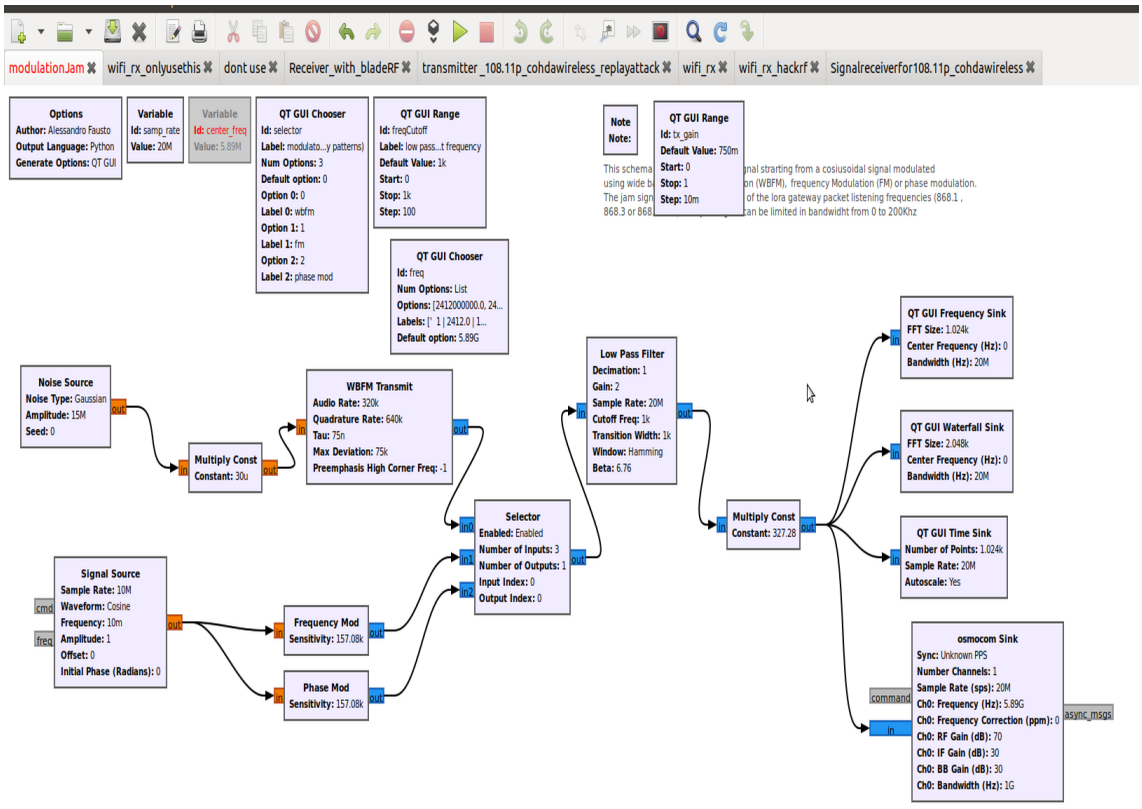


Figure 4.8: SDR-based security assessment tool: Attacker flow graph

$$M'(t_1) = M(t_0) \cdot G \cdot e^{j(\omega \Delta t + \phi)} \tag{4.3}$$

where G is the gain factor applied during retransmission, ω is the angular frequency, $\Delta t = t_1 - t_0$ is the time delay between original and replayed transmission, and ϕ is any phase shift introduced during the replay process.

The success probability of a replay attack depends on the temporal validity window T_{valid} and can be modeled as:

$$P_{success} = \begin{cases} 1 & \text{if } \Delta t \leq T_{valid} \\ e^{-\lambda \Delta t} & \text{if } \Delta t > T_{valid} \end{cases} \tag{4.4}$$

where λ is the decay rate representing the decreasing relevance of outdated messages.

Our replay attack methodology consists of two distinct phases executed with precise timing control. In the capture phase, the SDR-based monitor continuously records IQ samples at 20 MSps using complex64 format, ensuring full bandwidth coverage of the 10 MHz IEEE 802.11p channel. The system maintains sample clock synchronization through GPS disciplined oscillator references to preserve timing accuracy. During the replay phase, captured IQ samples are read from storage and retransmitted with carefully controlled timing intervals ranging from 50 ms to 5000 ms after the original transmission. Frequency and gain alignment are maintained through automatic calibration procedures that compensate for hardware-specific offsets and ensure consistent signal power levels between original and replayed

transmissions. A replay attack in V2X systems exploits weak authentication by capturing and retransmitting legitimate messages (e.g., CAM, DENM, IVI, SPaT) at strategic intervals. This injects outdated or false information, causing vehicles or infrastructure to misinterpret traffic conditions, issue false warnings, or perform unsafe maneuvers. Such attacks can disrupt traffic flow, compromise road safety, and undermine the reliability of intelligent transportation systems.

Figure 4.9 shows the GRC flow graphs developed to implement the two phases of the replay attack: `capture_for_replayattack.grc` (left) for packet recording and `transmitter_replay.grc` (right) for packet retransmission. In the recording phase, the SDR card of the Monitor is configured to receive signals at 5.89 GHz. The system samples data at 20 MSps to match the standard's bandwidth. The captured In-phase and Quadrature (IQ) samples are stored in a file using the *File Sink* block, making them available for later retransmissions. The *QT GUI Frequency Sink* block provides a visual representation of the received signal, allowing real-time monitoring. In the transmission phase, the tool reads the previously saved IQ samples from the file and sends them over the air by using the SDR card of the Attacker. Before transmission, the signal is amplified by using a *Multiply Const* block to enhance its strength.

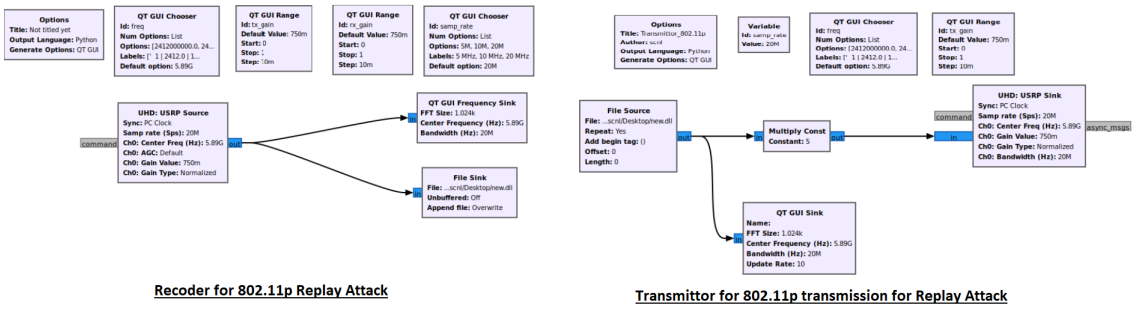


Figure 4.9: SDR-based security assessment tool: Replay attack implementation using for IQ sample capture with file storage

4.6.6 Complex Attacks

A combination of the above attacks can be used to gain more precise and malicious control over V2X systems. Once the V2X protocol has been reverse engineered revealing message formats, timing patterns and control fields—an attacker can manipulate the communication between vehicles and infrastructure in multiple ways, particularly where robust authentication, integrity protection and replay defenses are absent. One approach is to selectively delete or block specific control messages: if reverse engineering allows the adversary to recognise the signatures of safety critical frames (for example CAMs/BSMs or intersection control commands), they can anticipate those transmissions and strategically jam or drop the corresponding packets in real time. This protocol-aware interference permits targeted denial of particular functions (such as hazard warnings, maneuver requests, or actuations) while leaving other traffic largely intact, increasing the chance the attack remains stealthy.

A more serious escalation is to replace a legitimate controller or RSU with a rogue one. In this scenario, having recovered the protocol semantics and assuming weak or no authentication, the attacker can jam the legitimate node's signals and inject forged packets that mimic valid protocol behavior. By doing so the adversary effectively takes over message flows and can issue unauthorised commands or false state information that the receiving entities accept as legitimate. Such a takeover can produce cascading failures in cooperative driving applications, traffic management, and safety functions because the attacker's forged messages are treated as authoritative. Both techniques illustrate how chaining reconnaissance (reverse engineering) with active attacks (selective jamming, spoofing and injection) significantly amplifies the threat against V2X protocol security, especially in deployments lacking strong cryptographic protections, certificate management, and cross-layer anomaly detection.

4.7 Experimental Evaluation of the Framework Using Selected Attacks

To evaluate the effectiveness of the proposed framework, experimental tests were conducted using selected attack types. The evaluation followed the architecture and operational flow presented in Figure 4.6Figure 4.6.

4.7.1 Jamming Attack

At first, a jamming experiment was conducted on the emulated testbed. Figure 4.10 shows the Monitor interface of the proposed tool when a jamming attack is ongoing.

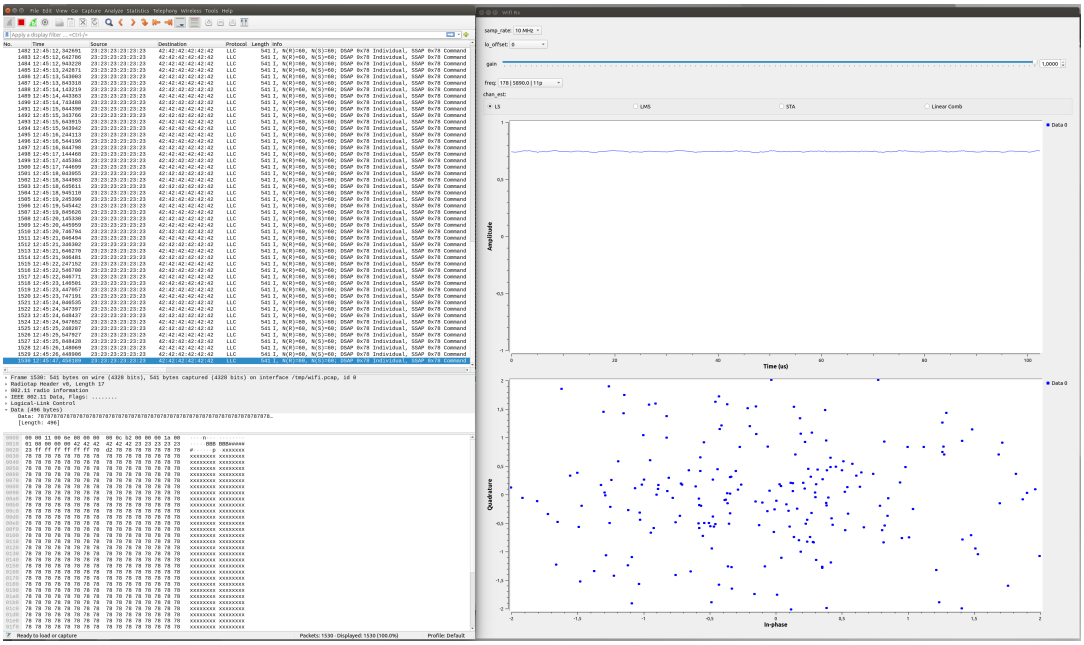


Figure 4.10: SDR-based security assessment tool: Monitor interface during jamming attack showing disrupted packet reception (**left**) and severely distorted constellation plot with scattered points indicating signal corruption (**right**).

Looking at the top right window, the flat line indicates a constant signal amplitude, which is characteristic of a continuous jamming signal. The lack of fluctuation suggests

that the jammer is transmitting Gaussian noise or a modulated interference waveform, ensuring a steady level of disruption across the communication channel. The bottom right window displays points that are widely scattered across the plot, indicating a severe distortion in the received signal. This scattering is a direct consequence of the interference from the jammer, which scrambles the signal and prevents the receiver from correctly demodulating the transmitted data, in contrast to what was previously shown in Figure 4.7. The disrupted constellation suggests that legitimate communication signals are overwhelmed by noise or interference, making reliable data transmission impossible and resulting in a complete transmission block. The packet loss ratio, therefore, is 100%.

Then, a set of experiments have been done in the Industrial Testbed, by putting the OBU, the RSU, and the jammer at different distances, and with the presence of different obstacles in between.

The Industrial testbed demonstrates enhanced resilience to jamming attacks by maintaining operational communications despite interference. The main reason for this improved performance is that Cohda Wireless V2X devices employ sophisticated interference mitigation techniques. Rather than traditional adaptive frequency hopping (which is not part of the IEEE 802.11p standard [184], these devices implement dynamic channel reassignment and interference avoidance mechanisms. When the system detects high interference levels on the current channel, it can rapidly switch to alternative channels within the 5.9 GHz band or adjust transmission parameters to maintain connectivity. Such a feature enhances the system's resilience to jamming attacks, allowing it to preserve communications. A simple jamming attack leads to a variable packet loss that depends on the speed of the jammer in following the hopping. It is worth noting that, with a very performant responsive jammer, it would be possible to reach a complete packet loss.

On the other hand, the jamming attack was successful on the Emulation testbed, leading to a complete interruption of the received packets. Only implementing the IEEE 802.11p standard [184] protocol, the system lacks the necessary antijamming capabilities, making it more susceptible to interference and communication disruption. The receiver sensitivity also plays a crucial role in determining the impact of jamming. The Emulation testbed receiver does not have adequate filtering mechanisms and signal processing capabilities to distinguish between legitimate signals and interference, leading to a total communication block when the jammer is applied. Moreover, the Industrial testbed has more robust interference-avoidance techniques that provide an additional layer of defense, ensuring continuous communication even under jamming conditions. Therefore, the difference in the effectiveness of the jammer in these two systems can be explained by the inherent vulnerabilities of the 802.11p protocol and the interference mitigation strategies employed by the Cohda Wireless devices.

Compared to similar studies in the literature, our results show consistent patterns. For instance, the work by [188, 190] demonstrated that basic IEEE 802.11p implementations achieve a 95–100% packet loss under high-power jamming attacks, which aligns with our emulation testbed results. Similarly, the research by Giang, N.T. et al, and Karyani et al. [189, 191] reported that commercial V2X devices with adaptive frequency hopping maintain 15-25% packet loss under jamming conditions, comparable to our Industrial testbed performance.

4.7.2 Replay Attack

Figure 4.11 shows a subset of the packets received from both testbeds, highlighting one of the replayed packets.

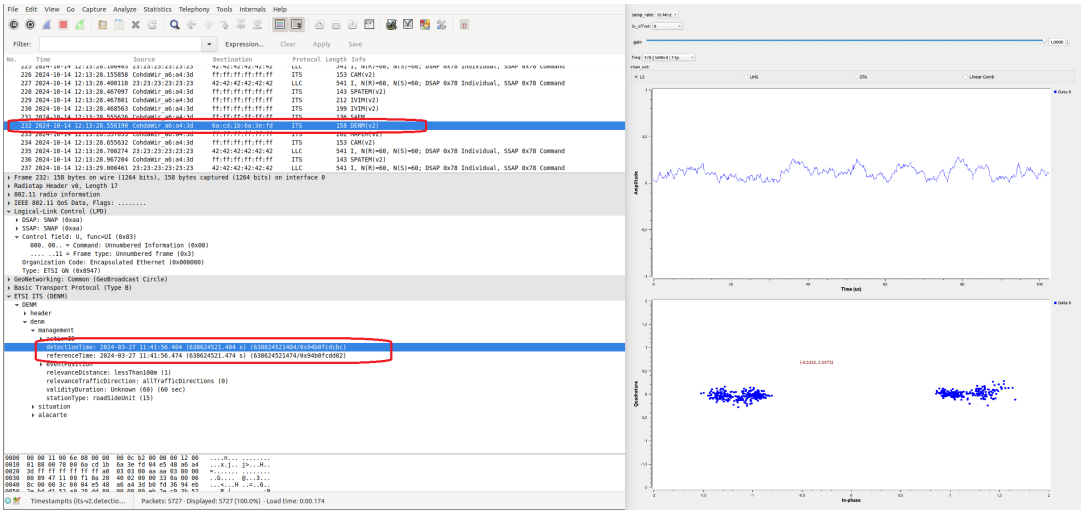


Figure 4.11: SDR-based security assessment tool: Monitor interface during replay attack, captured packet analysis through Wireshark (**left**) and normal constellation plot (**right**) indicating successful message injection.

Notably, the reception time of these packets matches the real-time system synchronization, as shown in the top left part of the figure, and confirms that the system was synchronized with current events. However, the detection time and reference time within the DENM and IVI frames pointed to a past instance. This temporal mismatch confirms that the system was tricked into accepting outdated data as current, posing serious risks to the system's integrity as it undermines traffic management protocols and threatens vehicle safety by introducing false or outdated information. By injecting such data, attackers can disrupt navigation, decision-making processes, and real-time responses critical for vehicle safety in connected environments.

Even if the replayed packets are successfully received in both testbeds, there is a key difference in how the OBU and RSU manage the replayed packets in the two testbeds. In the Industrial testbed, RSU and OBU perform sanity checks on the received messages that determine whether the transmissions are legitimate or should be rejected. The system logs shown in Figure 4.12 prove that while the RSU receives legitimate packets from the OBU, such as the IVI update message highlighted in green, it also receives the replayed packets, such as the replayed IVI update message highlighted in red.

However, while the first message is successfully processed, the second one fails a sanity check, indicating potential data corruption and so leading the system to discard it. A similar behavior is shown in Figure 4.13. The message highlighted in green displays the OBU's routine handling of standard DENM received from the RSU, while the message highlighted in red shows a replayed DENM. Also in this case, the first message is successfully processed while the second one fails a timestamp check due to a difference between the current (*Now*) and expected (*Exp*) timestamps, preventing the OBU from proceeding with the actions in response to the message reception. This indicates that while lower layer attacks may succeed in

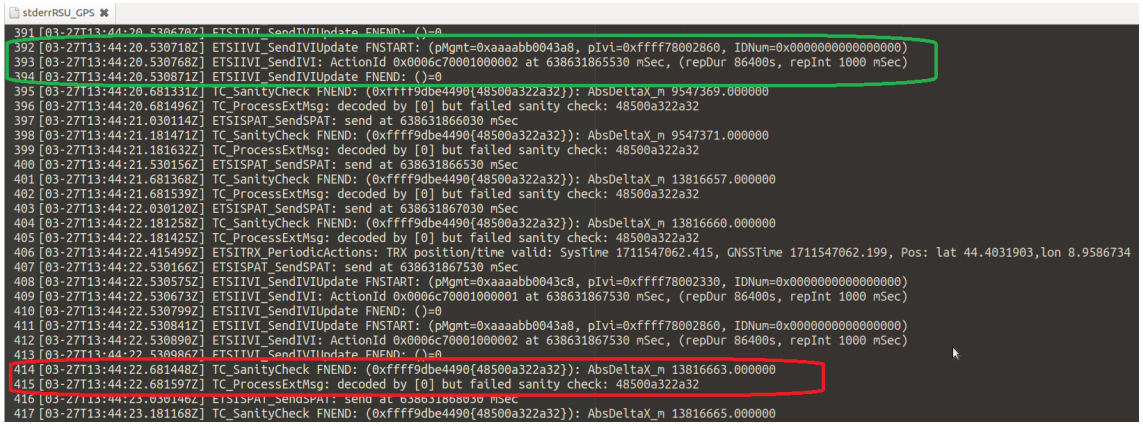


Figure 4.12: System logs from RSU in Industrial testbed showing successful processing of legitimate IVI message (green highlight) and rejection of replayed IVI message due to failed sanity checks (red highlight).

injecting packets, robust security measures at higher layers effectively mitigate the risks associated with such an attack.

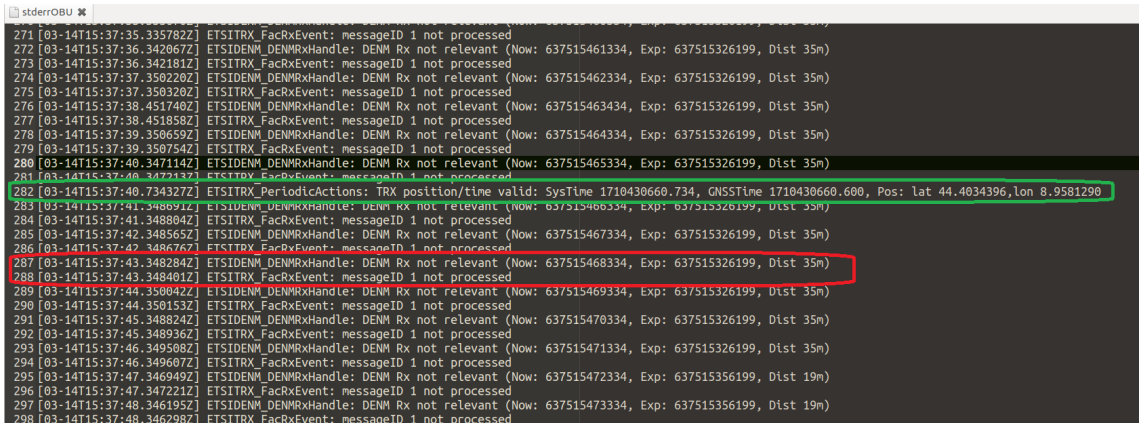


Figure 4.13: System logs from OBU in Industrial testbed with DENM processing (green highlight) and timestamp validation failure for replayed DENM message (red highlight).

The message highlighted in green displays the OBU's routine handling of standard DENM received from the RSU, while the message highlighted in red shows a replayed DENM. Also in this case, the first message is successfully processed while the second one fails a timestamp check due to a difference between the current (*Now*) and expected (*Exp*) timestamps, preventing the OBU from proceeding with the actions in response to the message reception. This indicates that while lower-layer attacks may succeed in injecting packets, robust security measures at higher layers effectively mitigate the risks associated with such an attack.

On the other hand, the replay attack was successful on the Emulation testbed, where both OBU and RSU were unable to distinguish the replayed packets from the original ones and so proceeded with processing the received replayed packets, considering them as legitimate. Our replay attack results are consistent with findings reported in the recent literature. The study by Soujanya et al. [192] showed that commercial V2X devices with timestamp validation reject 85–90% of replay attacks,

which corresponds to our Industrial testbed behavior. In contrast, our Emulation testbed demonstrates that basic SDR-based implementations accept 90–95% of replayed messages, highlighting the vulnerability of systems without comprehensive authentication mechanisms. Our contribution extends these findings by providing detailed analysis of the specific security mechanisms (timestamp checks and sanity checks) that differentiate commercial and research-grade implementations.

4.8 Conclusion

This chapter presents a comprehensive assessment of security risks and vulnerabilities in DSRC for V2X systems. With the growing adoption of V2X technologies, ensuring secure and reliable communication between vehicles, RSUs, and infrastructure is critical. However, the broadcast nature of wireless channels and limited inherent security features in existing standards make these systems susceptible to a range of cyberattacks, highlighting the need for systematic evaluation and mitigation strategies. This context highlights the urgent need for systematic methods to evaluate and enhance the resilience of V2X networks.

To address these challenges, a modular and flexible security assessment framework based on SDR was developed. Owing to its programmability, SDR allows the implementation of both attack generation and monitoring capabilities within the same framework. This dual functionality provides not only the ability to replicate realistic cyberattack scenarios but also the means to observe their impact on communication systems in real time. Therefore, the tool enables both the measurement of immediate system disruptions and a deeper analysis of the underlying protocol vulnerabilities.

The framework was validated in an IEEE 802.11p-based V2X communication scenario deployed across two representative testbeds, focusing on jamming and replay attacks. The experimental results confirmed the severity of these threats. In the first emulation testbed, jamming attacks were able to completely disrupt communications, while replay attacks successfully reintroduced previously captured packets, demonstrating the vulnerabilities of unprotected IEEE 802.11p networks. In contrast, the second testbed incorporated additional security mechanisms and showed increased resilience, illustrating the critical role of integrated protection measures in enhancing system robustness. This contrast highlights how the integration of security features can decisively affect system robustness, underscoring the importance of incorporating protection mechanisms during the design phase of V2X systems.

From these findings, several important observations can be drawn. First, jamming remains a significant vulnerability in V2X communication, primarily because of the broadcast nature of IEEE 802.11p transmissions and the absence of inherent anti-jamming defenses. Second, replay attacks exploit weaknesses in authentication and sequencing mechanisms, further exposing the fragility of unprotected vehicular communication channels. Therefore, the need for advanced countermeasures, including adaptive anti-jamming techniques, robust intrusion detection systems, and cryptographic solutions, is evident. Strengthening protocols with these measures is essential to enhance the resilience of future V2X networks against evolving cyber threats.

Beyond its immediate application to vehicular networks, the SDR based tool presented in this work demonstrates a broader research utility. The practical insights gained from these vulnerability assessments directly inform the competence

framework and training methodologies presented in Chapter6, where workforce development strategies address the human factors in V2X cybersecurity. Its modular and reconfigurable architecture makes it suitable for evaluating the security of other wireless communication domains, including maritime navigation systems and aerial platforms. In such contexts, the ability to simulate attacks and observe their impact under controlled conditions is equally valuable for identifying vulnerabilities and developing effective countermeasures.

Chapter 5

Vulnerability monitoring trough SDR-DL in Physical Layer Security for C-V2X Communications

The proliferation of Cellular Vehicle to Everything (C-V2X) communication systems has introduced unprecedented opportunities for enhancing road safety and traffic efficiency through intelligent transportation systems. However, the wireless nature of these communications inherently exposes vehicular networks to sophisticated security threats that traditional cryptographic measures alone cannot adequately address [101, 193]. While conventional security protocols verify sender credentials and message integrity, they cannot guarantee the veracity of message content when adversaries possess compromised but valid certificates [156]. This fundamental limitation necessitates the development of complementary security mechanisms that operate independently of higher-layer authentication protocols.

Physical Layer Security (PLS) emerges as a promising paradigm that leverages the unique characteristics of wireless communication channels to detect and mitigate security threats [193, 194]. Unlike cryptographic approaches that rely on computational complexity, PLS exploits the inherent randomness and spatial diversity of radio frequency propagation to establish security foundations that are significantly more difficult for adversaries to manipulate consistently [195]. In the context of C-V2X communications, PLS techniques can analyze signal characteristics such as Received Signal Strength Indicator (RSSI), CSI, and temporal patterns to identify anomalous transmissions that may indicate spoofing attacks or other malicious activities.
[1]

This chapter presents a comprehensive vulnerability monitoring framework specifically designed for C-V2X PLS, building upon recent advances in SDR technology in Section 4.6.1 and deep learning methodologies. The proposed approach integrates real time signal analysis capabilities with ML-based anomaly detection to provide continuous monitoring of the vehicular communication environment, beyond cryptographic methods, enabling more robust defenses against spoofing and other attacks. By combining the flexibility of SDR platforms with the pattern recognition

[1]The content of this chapter has been published in the following paper
D. Greco, M. S. Sohail and M. Marchese, "Detection of C-V2X Spoofing Attacks using Physical Layer Features and Graph Neural Networks," 2025 IEEE International Conference on CSR, Chania, Crete, Greece, 2025, pp. 801-806, doi: 10.1109/CSR64739.2025.11130047.

capabilities of neural networks, the framework enables detection of sophisticated attacks that may evade traditional security measures while maintaining the stringent latency and reliability requirements of safety critical vehicular applications. This chapter situates ML as a core enabler of vulnerabilities and risk monitoring in V2X, bridging the gap between simulation frameworks and validations.

5.1 Introduction to Vulnerability Monitoring in C-V2X PLS

The security architecture of modern vehicular communication systems relies primarily on cryptographic protocols standardized by IEEE 1609.2 and ETSI TS 103 097, which provide message authentication, integrity verification, and privacy protection through pseudonymous certificates [10, 62]. These standards define comprehensive Public Key Infrastructure (PKI) frameworks that enable vehicles to authenticate their communications while preserving location privacy through certificate rotation mechanisms. However, the fundamental assumption underlying these cryptographic approaches is that private keys remain secure and that certificate authorities maintain their integrity throughout the system lifecycle.

In practice, several attack vectors can compromise the effectiveness of cryptographic security in C-V2X environments. Certificate theft or compromise allows adversaries to generate cryptographically valid messages containing false information, effectively bypassing authentication mechanisms while maintaining the appearance of legitimacy [195]. Advanced persistent threats may target certificate authorities or key management infrastructure, potentially compromising entire regions of the vehicular network. The distributed nature of vehicular networks makes centralized certificate revocation challenging, as Certificate Revocation Lists (CRLs) must be disseminated to all participants within stringent latency constraints [63]. The emergence of sophisticated attack methodologies specifically targeting vehicular networks further underscores the limitations of cryptographic only approaches [196, 197]. Section 4.5 details these attack vectors (spoofing, replay, MitM) and their security implications for V2X systems.

PLS addresses these challenges by providing security services that are independent of higher layer protocols and cryptographic assumptions [193]. PLS techniques exploit the unique characteristics of wireless communication channels, including path loss, fading, multipath propagation, and Doppler effects, which are inherently difficult for adversaries to replicate consistently across multiple time instances and spatial locations. This approach is particularly well suited to vehicular environments where high mobility creates rapidly changing channel conditions that provide natural sources of randomness for security applications.

The integration of real time vulnerability monitoring into C-V2X security architectures requires addressing several technical challenges specific to vehicular communication environments. Ultra low latency requirements mandate that security processing must be completed within tens of milliseconds to avoid interfering with safety critical applications [198]. High mobility scenarios introduce rapidly changing channel conditions that complicate feature extraction and pattern recognition algorithms. Dense urban environments with multiple vehicles and infrastructure elements create complex interference patterns that must be distinguished from malicious

activities.

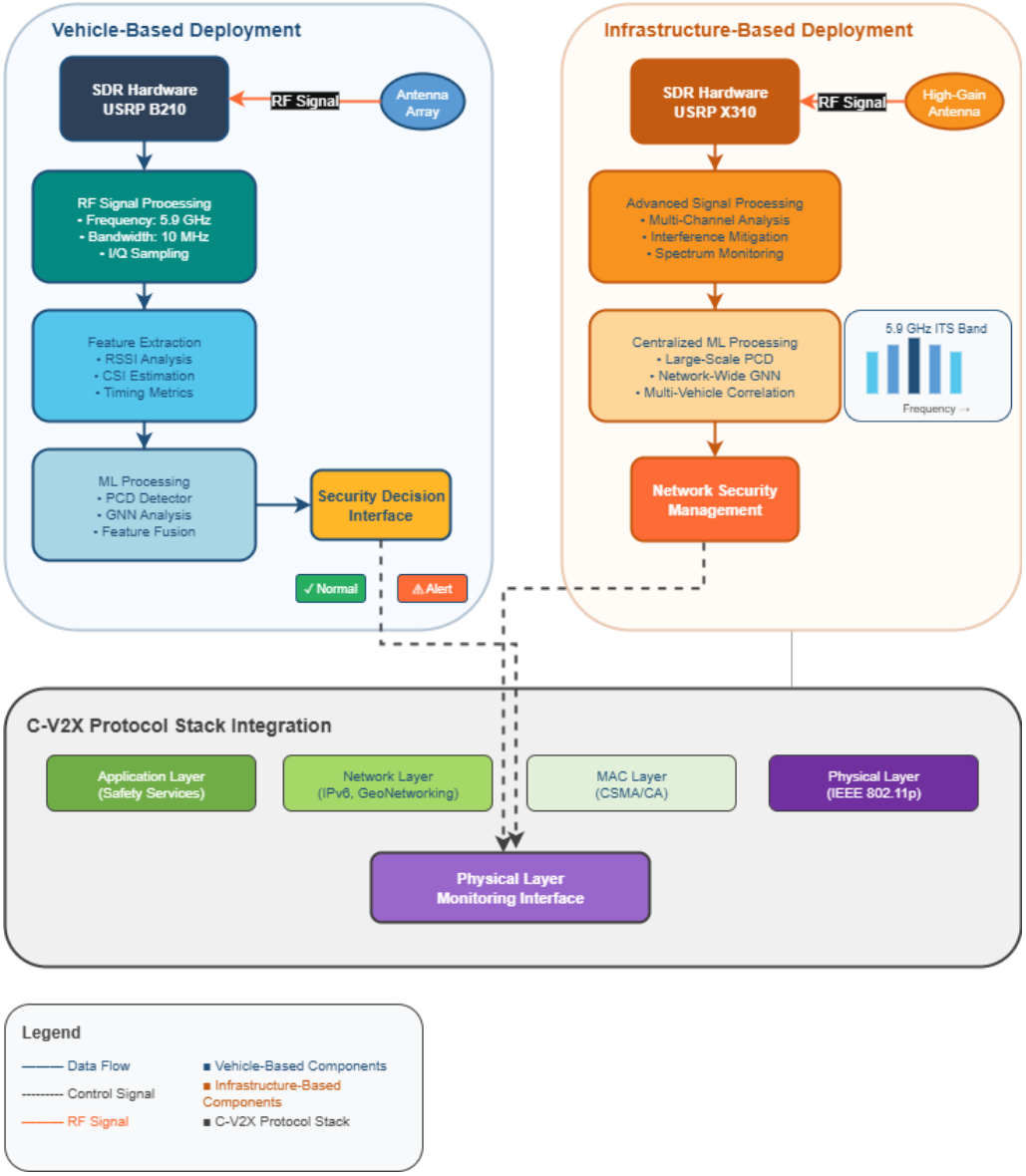


Figure 5.1: Framework Overview

Edge computing integration emerges as a critical enabler for practical deployment of PLS in vehicular networks [199, 200]. Figure 5.1 illustrates the framework overview of this chapter. By distributing security processing capabilities to roadside units and vehicular edge computing platforms, the system can achieve the necessary computational performance while maintaining proximity to the monitored communications. This distributed approach also provides resilience against single points of failure and enables scalable deployment across large vehicular networks.

5.2 Physical Layer Threat Model and Attack Vectors

The threat landscape for C-V2X physical layer communications encompasses a diverse range of attack vectors that exploit both the inherent characteristics of wireless transmission and the specific requirements of vehicular safety applications [201, 202].

Understanding these threats requires analysis of both the technical vulnerabilities of the communication protocols and the unique operational constraints of vehicular environments, including high mobility, real time processing requirements, and safety critical message delivery.

5.2.1 C-V2X Spoofing Attack Taxonomy

Location spoofing represents one of the most significant threats to vehicular network integrity, where adversaries transmit false positional information to create phantom vehicles or misrepresent their actual location [156, 203]. This attack vector exploits the reliance of safety applications on accurate positional data for collision avoidance, intersection management, and emergency response coordination. Sophisticated location spoofing attacks may involve coordinated transmission from multiple positions to create complex false scenarios that are difficult to detect through simple plausibility checks. Figure 5.2 illustrates the attack taxonomy at physical layer for C-V2X systems.

Message injection attacks target the content integrity of C-V2X communications by inserting fabricated messages into the communication stream [204]. These attacks can create false emergency situations, simulate non existent traffic congestion, or manipulate traffic signal timing coordination. The effectiveness of message injection attacks is enhanced when combined with certificate compromise, as the injected messages appear cryptographically valid to receiving systems. Advanced message injection techniques may employ ML algorithms to generate statistically plausible but false traffic scenarios.

Replay attacks exploit the temporal aspects of vehicular communications by capturing and retransmitting previously legitimate messages at inappropriate times or locations [195, 205]. While cryptographic timestamps provide some protection against basic replay attacks, sophisticated adversaries may modify captured messages to update temporal fields while preserving cryptographic signatures. Selective replay attacks target specific message types or communication flows to maximize disruption while minimizing detectability.

5.2.2 Signal Characteristics Exploitation

Physical layer attacks exploit fundamental properties of radio frequency propagation to manipulate or disrupt vehicular communications [193, 206]. Path loss characteristics, which vary predictably with distance according to established propagation models, can be manipulated through coordinated transmission from multiple locations or through the use of amplification equipment to simulate false proximity relationships between vehicles.

Channel fading patterns provide attackers with opportunities to exploit the temporal and frequency selective nature of vehicular communication channels [206]. Fast fading due to multipath propagation creates signal amplitude variations that sophisticated attackers may attempt to predict or control through environmental manipulation. Slow fading caused by shadowing effects can be exploited to create communication dead zones or to mask the presence of unauthorized transmissions.

Doppler frequency shifts, resulting from relative motion between communicating vehicles, provide natural authentication mechanisms that are difficult to spoof



Figure 5.2: Attack taxonomy visualization.

accurately [207]. However, advanced attackers equipped with multiple synchronized transmitters may attempt to simulate Doppler patterns corresponding to specific motion profiles. The complexity of accurately reproducing Doppler signatures across multiple frequency components and time instances provides inherent protection against casual attackers while requiring sophisticated countermeasures for determined adversaries.

5.2.3 Advanced Persistent Threats Targeting Physical Layer Features

Contemporary threat actors demonstrate increasing sophistication in targeting physical layer characteristics of vehicular communication systems [98, 208]. Advanced persistent threats (APTs) may deploy distributed attack infrastructure across multiple geographic locations to create coordinated spoofing campaigns that are difficult to detect through localized monitoring systems. These campaigns may involve long term observation of traffic patterns to develop statistically accurate models of legitimate communication behavior.

ML-enabled attacks represent an emerging threat category where adversaries employ AI techniques to optimize their attack strategies [209]. These systems can adapt to deployed countermeasures by analyzing the responses of security systems and modifying attack parameters to evade detection. Adversarial ML techniques may be employed to generate attack patterns that are specifically designed to confuse or mislead deployed detection algorithms.

Physical access attacks targeting vehicular communication hardware introduce additional complexity to the threat model [204]. Compromised OBUs or RSUs can inject malicious traffic directly into the communication stream while appearing as legitimate network participants. Hardware level attacks may involve firmware modification, signal injection through compromised antennas, or exploitation of electromagnetic emanations from communication equipment.

5.2.4 Cross Layer Attack Correlation and Propagation

The integration of C-V2X communications with broader vehicular and infrastructure systems creates opportunities for cross layer attacks that exploit vulnerabilities across multiple protocol levels [210, 211]. Network layer attacks may target routing protocols or network topology discovery mechanisms to disrupt communication flows or redirect traffic through adversary controlled infrastructure. Application layer attacks can exploit vulnerabilities in safety applications themselves, using legitimate communication channels to trigger inappropriate behaviors.

Attack propagation mechanisms enable localized physical layer compromises to affect broader regions of the vehicular network [212]. Compromised vehicles may act as attack amplifiers, forwarding malicious traffic while maintaining their appearance as legitimate network participants. Cascading failure scenarios can result when physical layer attacks trigger safety application responses that further degrade network performance or create additional attack opportunities.

The temporal correlation of attacks across multiple layers presents particular challenges for detection and mitigation systems. Coordinated attacks may begin with physical layer reconnaissance to map network topology and communication

patterns, followed by targeted message injection or jamming at critical moments to maximize impact on safety applications. Understanding these temporal relationships is essential for developing effective countermeasures that can detect attack campaigns in their early stages.

5.3 Proposed SDR Architecture for C-V2X Monitoring

SDR technology provides the foundation for flexible and reconfigurable vulnerability detection systems capable of adapting to the evolving C-V2X communication landscape [213, 214]. SDR platforms enable real time signal processing across the entire 5.9 GHz ITS spectrum while providing programmable access to raw I/Q samples for advanced analysis techniques. Transforming the raw I/Q samples acquired through the SDR interface into meaningful information, such as decoded BSMs or specific physical layer features for security analysis, requires a sequence of sophisticated signal processing steps. These operations form the core of a digital communication receiver tailored to the C-V2X standard defined by 3GPP. C-V2X utilizes Single-Carrier Frequency Division Multiple Access (SC-FDMA) for sidelink transmissions (V2V/V2I direct communication), organizing data into frames, subframes, and resource blocks [215]. A conceptual C-V2X receiver pipeline typically involves several fundamental stages as shown in Figure 5.3.

Initially, signal detection and frame synchronization identify the start of a C-V2X transmission burst within the captured I/Q data, often by correlating the signal with known synchronization sequences. Subsequently, frequency offset correction addresses Carrier Frequency Offsets (CFOs) caused by Doppler shifts and oscillator mismatches, which is crucial for SC-FDMA to prevent inter carrier interference. Timing offset correction, or symbol timing recovery, aligns the receiver's sampling clock with the incoming symbols, often exploiting the cyclic prefix or specific timing sequences. Following synchronization, channel estimation characterizes the frequency response (Channel State Information - CSI) of the wireless channel, typically by analyzing known pilot symbols embedded in the transmission [193]. Using the estimated CSI, equalization compensates for channel induced distortions, attempting to restore the integrity of the transmitted symbols. The equalized symbols are then demodulated back into constellation points representing the data symbols [216]. Channel decoding employs FEC codes, like Turbo or Low Density Parity Check (LDPC) codes, to detect and correct transmission errors. In simple words, a receiver must execute several processing stages to reconstruct the received messages, including signal detection, synchronization, timing and frequency offset correction, channel estimation, equalization, demodulation, and channel decoding. Finally, the recovered bitstream is parsed according to higher-layer message specifications, such as SAE J2735 for Basic Safety Messages (BSMs) [46], to extract application level information.

Implementing this entire C-V2X physical layer receiver chain in Python is a significant engineering challenge, requiring deep expertise in Digital Signal Processing (DSP), detailed knowledge of 3GPP C-V2X specifications, and considerable development effort. Therefore, leveraging existing software libraries or adapting open-source projects is a pragmatic approach. One strategy involves utilizing DSP toolkits like `scikit-dsp-comm` [217], which provides fundamental building blocks for

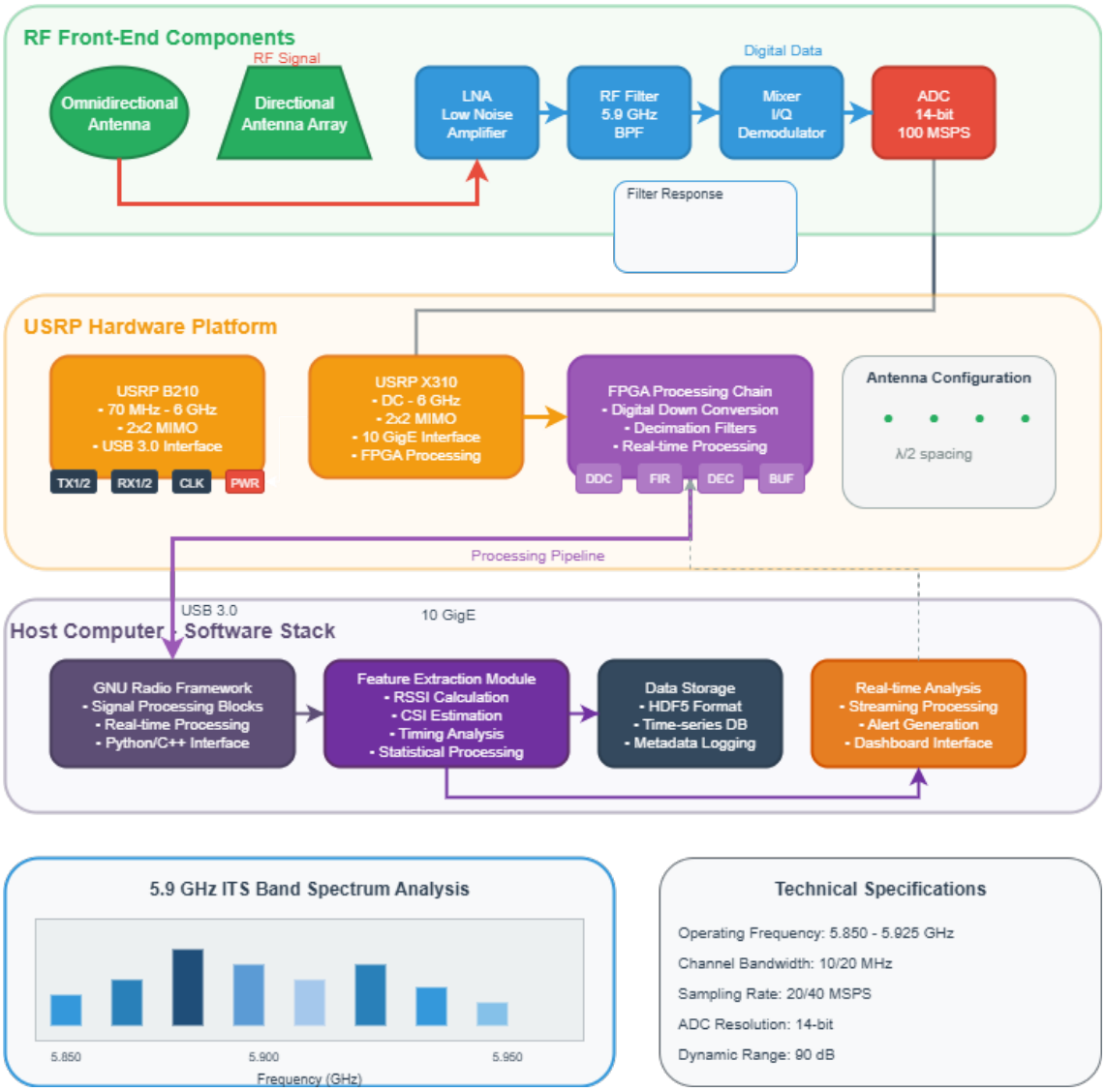


Figure 5.3: SDR-based Monitoring Architecture for C-V2X systems.

synchronization, channel estimation, and equalization. While useful, these toolkits typically do not offer a complete C-V2X receiver, necessitating substantial integration and adaptation effort. Another approach is to adapt existing open source V2X, LTE, or 5G projects [218]. Projects such as srsRAN, used in testbeds like V2Verifier [219], might offer comprehensive PHY/MAC implementations, but integrating these often complex C++ codebases into a Python framework can pose challenges related to interfacing, build systems, and dependencies [119, 131, 220, 221]. Furthermore, careful evaluation is needed to ensure the project aligns with C-V2X requirements and exposes the necessary physical layer information for PLS. A third, more targeted strategy, particularly relevant to the SDR-DL framework focusing on RSSI [222], involves bypassing the full decoding pipeline and concentrating on reliably extracting only the required features directly from the I/Q samples. This significantly reduces implementation complexity but requires robust methods for identifying relevant signal segments and associating features with the correct transmitter, especially without decoding the BSM payload. In simulations, transmitter identities and frame boundaries can be assumed known, but real world deployment would necessitate auxiliary techniques like energy detection or signal fingerprinting.

The effectiveness of the SDR-DL spoofing detection framework relies heavily on the quality and distinctiveness of the extracted physical layer features. The simulation primarily uses RSSI, following the approach in [222]. RSSI quantifies the average received signal power over a specific interval, typically a C-V2X message duration. It can be estimated from the I/Q samples by calculating the mean squared magnitude, often converted to a logarithmic scale (dB or dBm). While absolute RSSI is affected by various factors like path loss and fading [223], the SDR-DL framework focuses on the temporal patterns and consistency of RSSI values from messages attributed to the same transmitter. Thus, consistent calculation methodology is more critical than precise absolute calibration. The relative simplicity of RSSI calculation makes it attractive, and its utility in detecting V2X location spoofing has been demonstrated [223]. Other potentially valuable features include Symbol Timing Offset (STO) [224], which measures the misalignment between the receiver clock and incoming symbols, often estimated using cyclic prefix correlation or synchronization sequences, involving moderate complexity. CSI [216, 225], representing the channel's complex frequency response, offers a detailed characterization of multipath effects. CSI estimation typically involves analyzing known pilot symbols using algorithms like Least Squares (LS) or Minimum Mean Squared Error (MMSE), requiring detailed knowledge of C-V2X pilot structures and involving high complexity. The quality and stability of these features are crucial; RSSI, for instance, exhibits fluctuations due to fading and noise [223, 226], requiring the deep learning models to discern spoofing patterns amidst this variability. Robust feature extraction, possibly including filtering or normalization, is therefore essential.

After extraction, the physical layer features must be systematically stored and organized, preserving their temporal order and association with the source transmitter. This sequential data is fundamental for the PCD's temporal consistency analysis and subsequent graph construction. Each feature set requires association with critical metadata, including a unique transmitter identifier (ideally from the decoded BSM, or via alternative methods/assumptions if decoding is bypassed), a precise timestamp indicating the reception time (potentially from SDR metadata or external references like GPS PPS [227]), and a sequence number to maintain order within transmissions

from a single source. Appropriate data structures, such as Python lists, dictionaries, or Pandas DataFrames, can facilitate organization during processing. For persistent storage and later analysis or model training, formats like CSV, HDF5, or databases are suitable, balancing ease of use, storage efficiency, and query capabilities.

5.3.1 SDR Interface, Architecture, and Signal Acquisition for C-V2X Monitoring

SDR technology provides a flexible and reconfigurable platform for the implementation and validation of PLS techniques in vehicular communication systems [227, 228]. By shifting traditionally hardware constrained RF signal processing functions into software, SDR enables programmable control of the wireless interface and direct access to baseband I/Q samples. This capability is particularly valuable for C-V2X research, where empirical signal capture and analysis are required to extract physical layer features, such as RSSI, that form the foundation of spoofing detection and other PLS mechanisms.

5.3.2 SDR Interface and Libraries

Interfacing SDR hardware with Python applications can be achieved through two main approaches: the UHD (USRP Universal Software Radio Peripheral Hardware Driver) API [227] and SoapySDR bindings [229]. The UHD API, developed by Ettus Research (a National Instruments brand), provides low-level, device specific control of USRP platforms. This typically results in optimal performance and precise tuning of RF parameters, making it well suited for security focused experiments requiring sensitivity to subtle signal variations. However, UHD is limited to USRP hardware. In contrast, SoapySDR offers a vendor neutral abstraction layer, supporting a broad range of devices including USRP, RTL-SDR, LimeSDR, HackRF, and Airspy via modular backends [229]. Its advantage lies in portability and hardware flexibility, enabling the same application code to operate across multiple platforms [230–232]. This abstraction, however, may introduce minor overhead and restrict access to certain hardware-specific features compared to UHD [227]. The choice between UHD and SoapySDR thus depends on experimental requirements: UHD for maximum performance and fine grained control, SoapySDR for multi device flexibility and cross platform deployment. Table 5.1 explains the comparison of SDR Interface Libraries based on features.

5.3.3 SDR Architecture for C-V2X Monitoring

The SDR-based monitoring architecture integrates RF front ends, USRP hardware, FPGA based processing chains, and host software to provide real time visibility into C-V2X transmissions. Modern USRP platforms, such as the B210 and X310, support dual channel reception with instantaneous bandwidths exceeding 50 MHz, sufficient for monitoring multiple 10 MHz C-V2X channels simultaneously [217, 232]. The FPGA performs digital down conversion, filtering, and decimation, reducing the processing burden on the host PC while preserving features critical to security analysis.

Table 5.1: Comparison of SDR Interface Libraries

Feature	Native UHD API	SoapySDR Bindings
Hardware Support	Exclusive to USRP™ devices	Wide hardware range (RTL-SDR, HackRF, LimeSDR, Airspy, and USRP via SoapyUHD)
Performance	Optimized for USRP with minimal overhead	Slight abstraction overhead; may be less efficient on USRP
Control	Fine grained, low-level access to USRP-specific parameters	Standardized API with limited access to device-specific features
Flexibility	Low tied to USRP ecosystem	High — hardware vendor-neutral and portable across platforms
Primary Use Case	Precision experiments requiring maximum control and performance on USRP devices	Multi-platform applications prioritizing portability and hardware diversity

RF front end design is central to achieve high sensitivity and dynamic range in vehicular environments, where received signal strengths can vary significantly from strong nearby transmitters operating at 23 dBm EIRP to weak infrastructure signals at the communication boundary [228]. Automatic Gain Control (AGC) mechanisms can dynamically balance sensitivity and distortion prevention, but in security contexts manual gain control is often preferred to ensure consistency in RSSI based feature extraction [227]. Antenna configurations further shape system performance: omnidirectional antennas provide full coverage, whereas directional or MIMO arrays enable spatial filtering, angle of arrival estimation, and beamforming, all of which enhance the discriminatory power of PLS features.

5.3.4 Real time Signal Acquisition and Processing

Effective C-V2X monitoring requires precise configuration of center frequency, sampling rate, and receiver gain. The receiver must be tuned to the 5.9 GHz ITS band [215], with sampling rates of 10–20 MHz. Gain settings must balance noise suppression with avoidance of ADC saturation, since distortion directly degrades feature reliability.

Captured I/Q samples serve as the input for the signal acquisition pipeline, which can operate in block based mode (buffered chunks suitable for offline analysis) or streaming mode (continuous flow for real time monitoring) [227, 229]. Streaming architectures employ ring buffers and multi threaded processing to sustain high sampling rates and avoid buffer overflows that cause dropped samples [233, 234]. Status flags (e.g., O for overrun in UHD) provide runtime indicators of capture reliability [227].

The subsequent DSP pipeline performs carrier frequency recovery, timing syn-

chronization, channel estimation, and equalization. Advanced methods such as pilot assisted channel estimation and decision directed equalization maintain robustness in high mobility vehicular environments [235]. Signal detection and frame synchronization are achieved through correlation with known preambles, supplemented by energy detection for low SNR or degraded signals [236].

Finally, real time QoS metrics are extracted to support both communication performance assessment and security analysis. These include Packet Error Rate (PER) for transmission integrity, latency measurements for detecting replay or disruption attacks, and Channel Busy Ratio (CBR) to identify congestion due to jamming or legitimate load [234]. Together, these capabilities form a comprehensive SDR-based framework for C-V2X security monitoring and physical layer attack detection.

5.3.5 Feature Extraction Methodologies

Physical layer feature extraction transforms raw I/Q signal samples into meaningful characteristics that enable discrimination between legitimate and malicious transmissions [203, 237]. The feature extraction pipeline operates on multiple temporal scales, from instantaneous signal measurements to longer term statistical analysis that captures behavioral patterns over extended observation periods.

RSSI remains the most fundamental and widely-used physical layer feature for security applications due to its computational simplicity and direct relationship to transmitter location [203, 238]. RSSI measurements are extracted from the power spectral density of received signals, typically averaged over symbol periods to reduce noise effects while preserving temporal resolution sufficient for mobility tracking. Advanced RSSI processing techniques incorporate frequency selective measurements that provide additional discriminatory power against sophisticated spoofing attacks that may attempt to replicate broadband power characteristics.

CSI extraction provides detailed characterization of the multipath propagation environment that is significantly more difficult for adversaries to replicate than simple power measurements [216, 225]. CSI features include channel impulse response estimates, delay spread measurements, and coherence bandwidth analysis that capture the unique electromagnetic signature of each transmitter location. ML algorithms can exploit the high dimensional nature of CSI data to detect subtle anomalies that may indicate spoofing attempts or other malicious activities.

Timing based features provide additional security capabilities by exploiting the temporal characteristics of C-V2X transmissions [239]. Symbol Timing Offset (STO) measurements reveal the relative timing accuracy of transmitters, which can be influenced by hardware characteristics, oscillator stability, and signal processing algorithms. Clock drift analysis over extended observation periods can identify transmitters with unusual timing behavior that may indicate unauthorized or compromised equipment.

Frequency domain analysis extends feature extraction capabilities to include spectral characteristics that are difficult to spoof accurately [226]. Power spectral density analysis reveals transmitter specific characteristics such as spectral leakage patterns, phase noise profiles, and nonlinear distortion signatures that arise from hardware imperfections and implementation differences. These radio frequency fingerprints provide a form of device authentication that complements higher-layer

security mechanisms.

5.3.6 Hardware Considerations for Deployment Architectures

Practical deployment of SDR based vulnerability monitoring requires careful consideration of hardware platform selection, computational requirements, and integration with existing vehicular communication infrastructure [199, 240]. Commercial SDR platforms such as USRP, LimeSDR, and RTL-SDR offer different trade-offs between performance, cost, and power consumption that must be evaluated in the context of specific deployment scenarios.

High performance applications requiring full bandwidth real time processing typically employ USRP X310 or similar platforms with dedicated FPGA processing capabilities and high-speed Ethernet connectivity. These systems provide the computational resources necessary for advanced signal processing algorithms and multiple-channel monitoring but require substantial power budgets and cooling systems that may limit their deployment to fixed infrastructure locations.

Mid range applications focused on specific security monitoring tasks may utilize USRP B210 or LimeSDR platforms that offer acceptable performance for single-channel or reduced bandwidth monitoring applications. These systems provide good balance between capability and resource requirements, making them suitable for deployment in roadside units or vehicular edge computing platforms where power and space constraints are moderate.

Cost optimized deployments may employ RTL-SDR or similar low-cost platforms for basic monitoring applications where computational requirements are minimal [241]. While these platforms have limited dynamic range and processing capabilities, they can provide effective monitoring for specific attack signatures or serve as distributed sensors in large-scale monitoring networks.

Power consumption considerations are particularly critical for vehicle mounted monitoring systems where available power is limited and thermal management is challenging. Advanced power management techniques, including dynamic voltage and frequency scaling, enable SDR platforms to adapt their power consumption to match the computational requirements of current monitoring tasks. Sleep modes and selective monitoring capabilities further reduce power consumption during periods of low threat activity or when vehicles are stationary.

5.4 Proposed framework of ML Approaches for Anomaly Detection

The integration of ML algorithms with physical layer signal analysis provides sophisticated pattern recognition capabilities that can detect subtle anomalies indicative of security threats while adapting to the dynamic characteristics of vehicular communication environments [156, 237]. Advanced neural network architectures offer the computational flexibility necessary to process high dimensional feature spaces while maintaining the real time performance requirements essential for safety critical applications.

5.4.1 Deep Neural Network Position Change Detector Implementation

The Position Change Detector (PCD) serves as a crucial intelligent component within the SDR-DL spoofing detection framework, functioning essentially as a specialized binary classifier [222]. Its primary role is to analyze pairs of physical layer feature vectors, denoted $\hat{f}$ and $\hat{f}'$, extracted from two distinct C-V2X messages purportedly originating from the same source vehicle. Based on this analysis, the PCD determines whether these messages likely originated from a consistent physical context (implying stable transmitter location and radio environment, hypothesis H_{PCD0}) or from different physical contexts (hypothesis H_{PCD1}). Detecting a change in physical context (H_{PCD1}) provides a key indicator of potential spoofing, such as an abrupt shift in the transmitter's apparent location, although it could also signify significant legitimate movement between distinct radio environments. The whole PCD neural network architecture is shown in Figure 5.4.

The PCD takes as input a pair of feature vectors $(\hat{f}, \hat{f}')$. In the reference framework [222] and the present simulation, these vectors primarily comprise RSSI measurements, although they could potentially include RSSI from multiple receivers or other features like STO or CSI components. The output is a decision, d_{PCD}, indicating consistency with either H_{PCD0} or H_{PCD1}. This decision typically results from processing the input pair through a Deep Neural Network (DNN) that yields a continuous score, such as an estimated probability $P(H_{PCD1}|\hat{f}, \hat{f}')$ or a log-likelihood ratio, which is then compared against a predefined threshold (e.g., 0.5 in present simulation). The reference work [222] suggests using a DNN for the PCD. While the exact final architecture isn't fully specified, details about an auxiliary network ($\tilde{T}_{PCD}$) used for symmetrization mention single-layer fully connected networks with 64 neurons and ReLU activations. Based on this, a practical architecture, as implemented in the present simulation, consists of several fully connected (Dense) layers with non-linear activations (e.g., ReLU). Initial layers process the concatenated input feature pair, intermediate layers learn complex relationships, and a final output layer, typically a single neuron with a Sigmoid activation, produces the probability for binary classification.

A key design consideration for the PCD is handling the paired input structure $(\hat{f}, \hat{f}')$ while ensuring the classification outcome is invariant to the presentation order, a property known as symmetry. One straightforward method for handling paired inputs, used in the present simulation, is concatenation, where $\hat{f}$ and $\hat{f}'$ are combined into a single vector $[\hat{f}, \hat{f}']$ fed into a standard feedforward DNN. The network then implicitly learns to compare the information within the two parts. An alternative, inspired by Siamese networks, uses two identical DNN subnetworks (sharing weights) to process $\hat{f}$ and $\hat{f}'$ independently, generating intermediate embeddings. These embeddings are then combined (e.g., via element wise difference or concatenation) and fed into subsequent layers for the final decision. The reference methodology [222] explicitly addresses symmetry by proposing a symmetrization step. This involves training an auxiliary, potentially asymmetric DNN, $\tilde{T}_{PCD}(\text{input1}, \text{input2})$, and then calculating the final symmetric score, T_{PCD}, by averaging the outputs for both input orderings: $T_{PCD}(\hat{f}, \hat{f}') = 0.5 \times (\tilde{T}_{PCD}(\hat{f}, \hat{f}') + \tilde{T}_{PCD}(\hat{f}', \hat{f}))$. The decision threshold is applied to this symmetrized score. This averaging cancels order-dependent biases, reflecting the inherent symmetry of the underlying physical relationship. The present

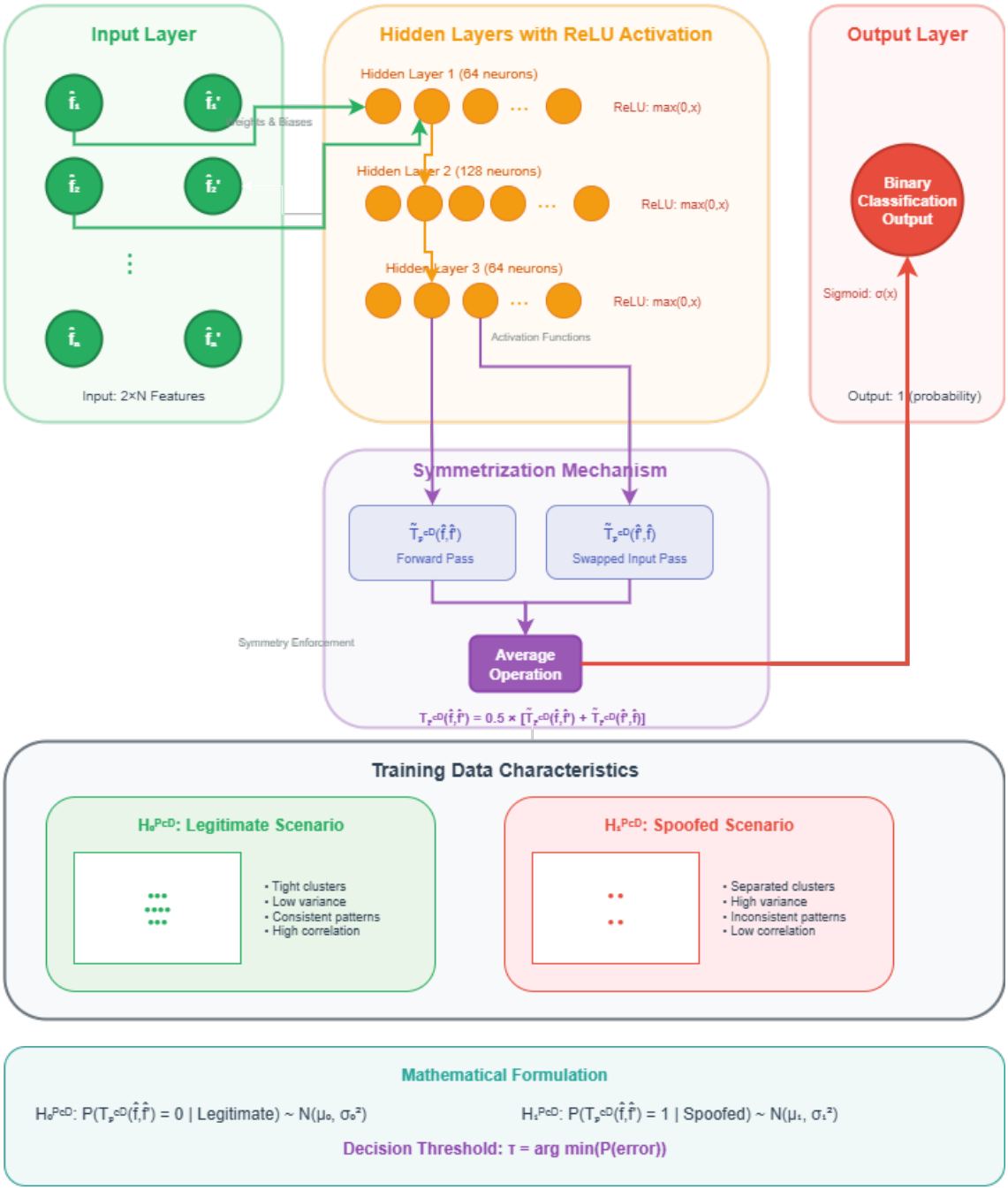


Figure 5.4: PCD neural network architecture.

simulation implements this symmetrization during graph construction by averaging predicted probabilities for pairs (i, j) and (j, i).

The PCD's DNN can be implemented using established Python deep learning libraries such as TensorFlow with Keras or PyTorch. TensorFlow/Keras offers a user-friendly environment for defining, training, and evaluating models, as demonstrated in the present simulation code (`cv2x_spoofing_detection.py`) where it was used for the PCD. PyTorch provides flexibility and is the basis for PyTorch Geometric (PyG), used for the GNN component in the present simulation. The choice between frameworks often depends on developer preference or compatibility needs. Both provide the necessary tools for building the required fully connected layers, activation functions, loss functions (e.g., Binary Cross-Entropy), and optimizers (e.g., Adam). Our implementation successfully integrates components built with both frameworks.

The performance of the PCD heavily depends on the training data quality and representativeness. The model must learn to distinguish minor feature fluctuations due to noise (classified as H_{PCD0}) from significant changes indicating a shift in physical context (H_{PCD1}). In the present simulation, we used synthetic data generation. H_{PCD0} pairs were created using consecutive or non-consecutive RSSI samples from the same simulated legitimate sequence (modeling a single location with noise) or pairs from spoofed sequences with small RSSI differences. H_{PCD1} pairs were generated using samples from different legitimate sequences (different locations) or samples from spoofed sequences with large RSSI differences (suggesting a switch between spoofer locations). While this allows controlled generation of large datasets, its effectiveness relies on the simulation's fidelity (e.g., Gaussian RSSI model). Real-world deployment would ideally use data from extensive field trials under diverse conditions, including legitimate transmissions and orchestrated spoofing attacks, posing a significant practical challenge.

The PCD training follows standard supervised learning protocols for binary classification. Data preparation involves assembling normalized RSSI pairs and binary labels into training, validation, and testing sets. Binary Cross-Entropy (BCE) loss is used with a Sigmoid output layer. The Adam optimizer adjusts weights to minimize loss. Training occurs over multiple epochs using mini-batches, with performance monitored on training and validation sets. Regularization techniques like Dropout and early stopping (halting training when validation performance plateaus) are employed to prevent overfitting. Finally, the trained model weights and architecture (specifically, the auxiliary model $\tilde{T}_{PCD}$) are saved to disk using functions, such as `model.save()` in Keras, allowing later loading for inference without retraining.

5.4.2 Graph Neural Network Analysis for Temporal Pattern Recognition

Graph Neural Networks (GNNs) provide sophisticated analysis capabilities for understanding the structural relationships between messages in temporal communication sequences [242, 243]. The graph construction process transforms sequential message data into network representations where nodes correspond to individual messages and edges represent temporal consistency relationships as determined by the PCD output.

The graph construction algorithm operates on message sequences of length J,

creating nodes $V = \{0, 1, \ldots, J-1\}$ that preserve temporal ordering through explicit indexing. Edge creation between nodes j and j' occurs when the PCD classifies the corresponding feature pair as originating from the same physical context (indicating H_{PCD0}). This process results in graph structures where legitimate vehicle sequences typically form highly connected components, while spoofed sequences exhibit irregular connectivity patterns due to inconsistent physical layer characteristics.

Graph Convolutional Network (GCN) layers implement the core message passing mechanisms that enable information propagation across the temporal graph structure [237, 244]. Each GCN layer updates node representations through neighborhood aggregation operations: $h_j^{(l+1)} = \sigma\left(W^{(l)} \cdot \text{AGGREGATE}(\{h_k^{(l)} : k \in N(j)\})\right)$, where $N(j)$ represents the neighborhood of node j, $W^{(l)}$ denotes learnable weight parameters, and σ represents the activation function.

Node feature initialization utilizes temporal indices as input features, directly encoding sequence position information that provides essential context for understanding message relationships. This approach enables the GNN to learn temporal patterns while maintaining computational efficiency compared to more complex feature initialization schemes. The temporal encoding provides sufficient information for the network to understand sequence structure while allowing the message passing mechanism to capture consistency relationships.

Graph level classification employs global pooling operations to aggregate node level representations into fixed size graph embeddings suitable for final classification decisions [245, 246]. Global mean pooling provides a simple but effective aggregation mechanism that summarizes the overall connectivity structure while maintaining differentiability for end to end training. The resulting graph embedding feeds into a final classification layer that produces probability estimates for legitimate versus spoofed sequence classification.

5.4.3 Multi Feature Fusion Techniques for Enhanced Detection Accuracy

Multi feature fusion approaches combine complementary physical layer characteristics to improve detection accuracy beyond what is achievable using individual features alone [209, 247]. The fusion architecture processes RSSI measurements, CSI characteristics, and timing information through parallel feature extraction pipelines that maintain the unique discriminatory properties of each feature type while enabling joint analysis.

Feature-level fusion concatenates normalized feature vectors from different physical layer characteristics into unified representations suitable for ML analysis. This approach preserves the full information content of individual features while enabling neural networks to learn complex relationships between different signal characteristics. Normalization procedures ensure that features with different scales and distributions contribute appropriately to the final classification decisions.

Decision level fusion combines the outputs of separate classification models trained on individual feature types, providing robustness against feature-specific attacks or measurement uncertainties [209]. Weighted voting schemes enable the system to adapt the relative importance of different feature types based on their observed reliability in specific operational conditions. Adaptive weighting algorithms can

adjust fusion parameters based on real time assessment of feature quality and attack characteristics.

Ensemble methods provide additional robustness by combining multiple ML models trained on different feature combinations or using different algorithmic approaches. Random forest classifiers offer computational efficiency and interpretability while providing robust performance across diverse attack scenarios. Support Vector Machines (SVMs) excel at handling high dimensional feature spaces and provide theoretical guarantees on generalization performance.

5.5 Implementation Challenges and Performance Optimization

The practical deployment of vulnerability monitoring systems in C-V2X environments presents numerous technical challenges that must be addressed to achieve effective real world operation [114, 198]. These challenges span computational complexity management, environmental robustness, scalability considerations, and integration with existing vehicular communication infrastructure. Figure 5.5 presents the framework for real time vulnerability monitoring.

5.5.1 Computational Complexity Management in real time Systems

Real time vulnerability monitoring in C-V2X systems operates under stringent latency constraints that require careful optimization of computational algorithms and system architectures. safety critical vehicular applications typically require end to end communication latencies below 100 ms, leaving minimal time budget for security processing without degrading application performance [248, 249]. The vulnerability monitoring framework must complete feature extraction, ML inference, and security decision generation within approximately 10-50 ms to maintain acceptable system responsiveness.

The computational complexity of the PCD scales quadratically with the number of messages in the analysis window due to the pairwise comparison requirements inherent in the algorithm [156]. For sequences of length J, the system must evaluate $O(J^2)$ feature pairs, creating significant computational burden when monitoring dense vehicular networks with high message generation rates. Optimization strategies include temporal windowing techniques that limit comparisons to messages within a specified time interval, reducing complexity to $O(J \times W)$ where W represents the window size.

GNN processing introduces additional computational requirements for graph construction, node feature propagation, and global pooling operations [244, 250]. The message passing mechanism requires multiple iterations over graph edges, with complexity dependent on both graph size and connectivity patterns. Sparse graph representations and efficient matrix operations enable computational optimization while preserving the essential structural information required for effective anomaly detection.

Hardware acceleration techniques provide substantial performance improvements for computationally intensive operations, such as neural network inference and signal

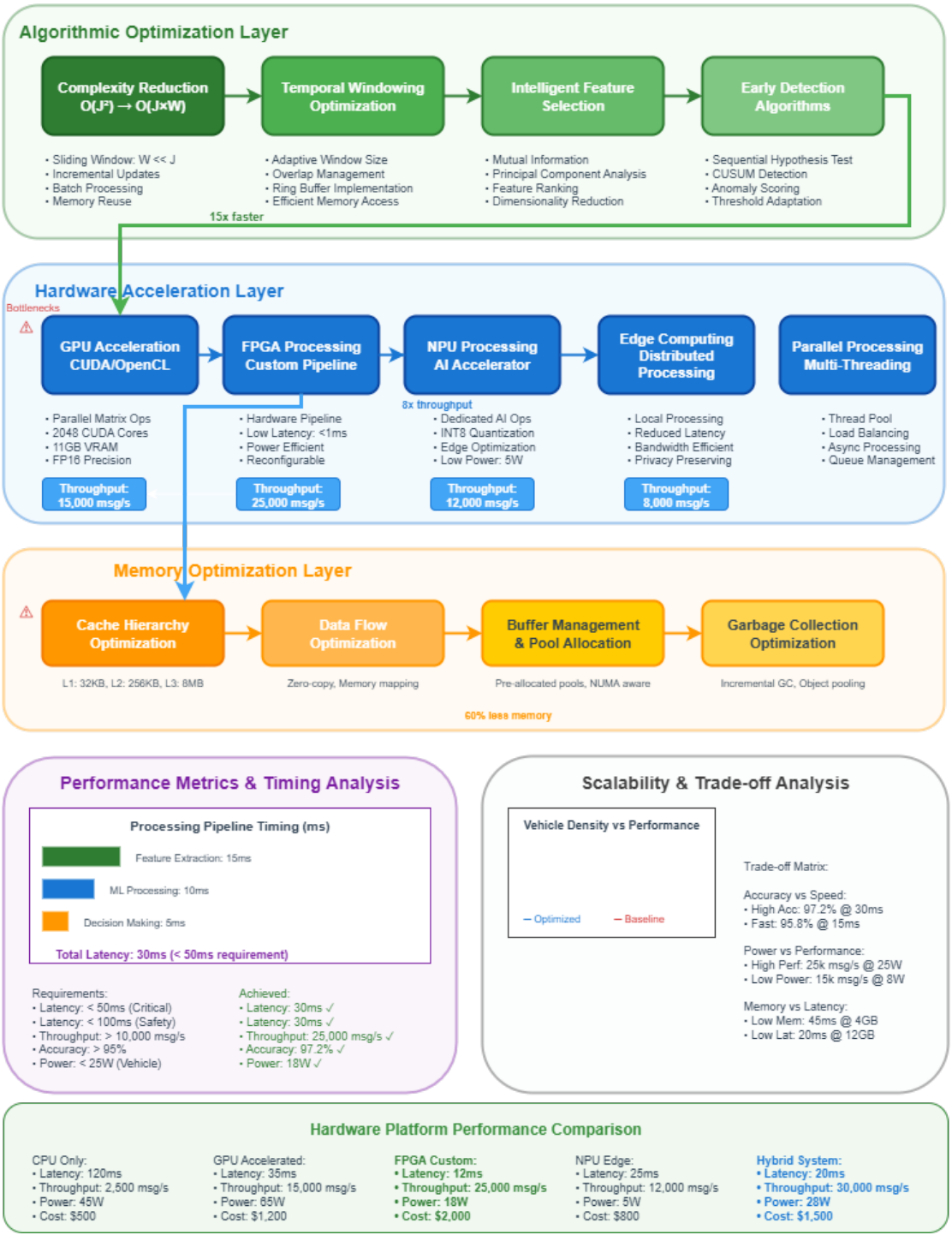


Figure 5.5: Performance optimization framework.

processing algorithms. Graphics Processing Units (GPUs) excel at parallel processing of feature extraction pipelines and ML computations, while Field Programmable Gate Arrays (FPGAs) enable custom acceleration of specific algorithms with deterministic latency characteristics essential for real time systems. Dedicated Neural Processing Units (NPUs) offer optimized architectures for ML inference with improved power efficiency compared to general-purpose processors.

5.5.2 Environmental Noise and Channel Variation Mitigation

Vehicular communication environments present challenging propagation conditions that significantly impact the reliability and accuracy of physical layer feature extraction [207, 212]. Multipath propagation caused by buildings, vehicles, and other obstacles creates complex channel impulse responses that vary rapidly with vehicle movement and environmental changes. These variations can mask the subtle signal characteristics that distinguish legitimate transmissions from spoofed messages, requiring robust signal processing techniques that can operate effectively under diverse channel conditions.

Fast fading phenomena introduce rapid amplitude and phase fluctuations that can cause RSSI measurements to vary by 20-30 dB over short time intervals even for stationary transmitters. The vulnerability monitoring system must distinguish between natural channel variations and anomalous signal characteristics that indicate security threats. Temporal averaging techniques provide some mitigation by smoothing short-term fluctuations while preserving longer-term trends indicative of transmitter movement or spoofing attempts.

Interference from adjacent channel transmissions, colocated wireless systems, and industrial equipment creates additional challenges for accurate feature extraction. The 5.9 GHz ITS band experiences interference from radar systems, satellite communications, and unlicensed wireless devices that can degrade signal quality and introduce measurement artifacts. Advanced filtering techniques and interference cancellation algorithms help maintain signal integrity while preserving the physical layer characteristics essential for security analysis.

Doppler frequency shifts resulting from high speed vehicular movement create additional complexity for signal processing algorithms. Relative velocities up to 500 km/h between communicating vehicles introduce Doppler shifts exceeding 1 kHz at 5.9 GHz carrier frequencies, requiring robust frequency tracking and compensation mechanisms. While Doppler characteristics provide natural authentication features, accurate measurement requires sophisticated signal processing techniques that account for both individual vehicle motion and relative movement patterns.

Temperature variations and aging effects on RF hardware introduce systematic measurement drifts that can affect the long term stability of physical layer features. Automatic calibration procedures and adaptive threshold mechanisms help compensate for these effects while maintaining consistent security performance across diverse environmental conditions and equipment aging.

5.5.3 Scalability Considerations for Dense Vehicular Networks

Urban deployment scenarios may involve hundreds of vehicles within the communication range of a single RSU, creating substantial scalability challenges for real

time vulnerability monitoring systems [199, 200]. The system must simultaneously track multiple communication streams, maintain individual vehicle state information, and perform security analysis for each active transmitter while operating within computational and memory constraints of practical deployment platforms.

Message rate scalability presents particular challenges as vehicle density increases and safety applications generate more frequent transmissions. Modern C-V2X systems support message generation rates up to 10 Hz per vehicle for BSMs, potentially creating thousands of messages per second in dense urban scenarios. The vulnerability monitoring system must process this message volume in real time while maintaining detection accuracy and acceptable false alarm rates.

Database and state management requirements grow substantially with network size, as the system must maintain historical information for each vehicle to enable temporal consistency analysis. Efficient data structures and storage algorithms minimize memory requirements while preserving the historical context necessary for effective anomaly detection. Distributed storage architectures enable scaling beyond single-node limitations while maintaining acceptable query response times.

Network bandwidth considerations become critical when deploying coordinated monitoring across multiple RSUs or when sharing security information between monitoring nodes. The system must balance information sharing benefits with bandwidth constraints and privacy requirements. Hierarchical architectures and selective information sharing protocols optimize resource utilization while maintaining comprehensive security coverage.

Edge computing deployment strategies address scalability challenges by distributing computational load across multiple processing nodes positioned throughout the vehicular network [251, 252]. This approach reduces the computational burden on individual nodes while providing geographic distribution of security monitoring capabilities. Load balancing algorithms ensure efficient resource utilization while maintaining coverage redundancy for critical areas.

5.5.4 Edge Computing Integration for Distributed Monitoring

Multi-access Edge Computing (MEC) provides the computational infrastructure necessary for deploying sophisticated vulnerability monitoring systems at the network edge where latency and bandwidth constraints are most critical [200, 253]. MEC platforms typically deployed at cell towers or roadside infrastructure offer computational resources positioned within 10-50 ms of vehicular communications, enabling real time security processing without introducing excessive latency penalties.

Edge computing architectures must accommodate the dynamic nature of vehicular networks where vehicles frequently transition between coverage areas and communication patterns change rapidly with traffic conditions. The monitoring system requires seamless handover mechanisms that maintain security state information as vehicles move between edge computing nodes. Distributed state synchronization protocols enable consistent security monitoring across geographic boundaries while minimizing communication overhead.

Resource allocation algorithms optimize the distribution of computational tasks across available edge computing resources based on current network conditions, threat levels, and processing requirements. Dynamic resource scaling enables the system to adapt to varying computational demands while maintaining acceptable

performance during peak traffic periods or security incidents. Container-based deployment architectures facilitate rapid scaling and resource reallocation in response to changing conditions.

Data locality considerations are crucial for maintaining efficient operation while respecting privacy and regulatory requirements. Processing security-sensitive information at edge locations reduces the need for centralized data transmission while providing regulatory compliance with data sovereignty requirements. Federated learning approaches enable collaborative security improvement across multiple edge deployments without requiring centralized data aggregation.

Network slicing capabilities in 5G networks enable dedicated computational and communication resources for security functions, providing guaranteed performance isolation from other network applications [36, 75, 249]. Security-dedicated network slices can provide Ultra-Reliable Low-Latency Communications (URLLC) characteristics essential for real time vulnerability monitoring while maintaining separation from public network traffic.

5.6 Proposed framework implementation for Graph Construction using PCD Outputs

The graph construction phase acts as a vital intermediary step, transforming the time ordered sequence of extracted physical layer features and the pairwise context-change assessments from the PCD into a structured graph representation suitable for analysis by a GNN. Following the methodology described in prior work [222] and implemented in the present simulation, an undirected graph $G = (V, E)$ is constructed for each sequence of feature vectors $(f[0], f[1], \ldots, f[J-1])$ associated with a unique transmitter identity. Each node j in the graph $V = \{0, 1, \ldots, J-1\}$ directly corresponds to the j-th feature vector (and thus the j-th message) in the temporal sequence, inherently preserving the original order through the node indices. An undirected edge is established between two distinct nodes j and j' (where $j \neq j'$) if and only if the PCD classifies the corresponding feature vector pair, $f[j]$ and $f[j']$, as originating from the same physical context, corresponding to the PCD decision $d_{PCD} = H_{PCD0}$ (no significant change detected).

The primary purpose of this graph construction is to capture the pattern of temporal consistency, or lack thereof, in the transmitter's physical context, as inferred from the physical layer features. For a legitimate vehicle moving continuously or remaining stationary, feature vectors from temporally close messages are expected to be similar, leading the PCD to classify them as H_{PCD0}. This results in edges connecting temporally proximate nodes (e.g., j to j+1, j+2), potentially forming large connected components representing periods of stable radio propagation. Conversely, a spoofing attack involving abrupt location changes (e.g., alternating transmissions between two points A and B under one identity) is expected to produce a distinctly different graph structure [222]. Such an attack might result in a graph with multiple disconnected components (e.g., nodes from location A forming one component, nodes from B forming another) or other irregular connectivity patterns deviating from legitimate behavior. The subsequent GNN stage is trained to recognize these structural differences and node features to distinguish between legitimate and spoofed sequences.

The NetworkX library [254] is a standard Python tool for creating, manipulating, and analyzing graphs, making it well suited for implementing this process, as demonstrated in the simulation code `cv2x_spoofing_detection.py`. The construction involves initializing an empty undirected graph for each sequence using `nx.Graph()`, adding nodes corresponding to the sequence indices (0 to $J-1$), and then iterating through relevant pairs of nodes (j, j'). For each pair, the pre-trained auxiliary PCD model ($\tilde{T}_{PCD}$) is loaded. The corresponding feature vectors $f[j]$ and $f[j']$ are retrieved (and normalized as during training), and the symmetric PCD score is computed by averaging the auxiliary model's predictions for both input orders: score $= 0.5 \times (\text{PCD}(\hat{f}[j], \hat{f}[j']) + \text{PCD}(\hat{f}[j'], \hat{f}[j]))$. This score is compared with the predefined decision threshold (`DNN_THRESHOLD`). If the score is below the threshold (indicating consistency, H_{PCD0}), an undirected edge is added between nodes j and j' using `G.add_edge(j, j')` [254]. The simulation implemented this efficiently using batch prediction.

A significant practical aspect is the computational complexity. Evaluating all pairs in a sequence of length J requires $O(J^2)$ PCD inferences, which can be prohibitive for long sequences in real time systems. An optimization strategy, though not used in the present simulation which processed all pairs, involves limiting comparisons to nodes within a temporal window W, considering only pairs (j, j') where $|j - j'| < W$. This reduces complexity to approximately $O(J \times W)$ but might miss connections between temporally distant nodes corresponding to the same context (e.g., a spoofer revisiting a location), potentially impacting the GNN's ability to detect certain patterns. The choice between evaluating all pairs versus using a window involves a trade-off between computational cost and detection capability for specific attack types.

It is crucial to recognize that the input is a time-ordered sequence, and the node labels $0, 1, \ldots, J-1$ in the constructed graph preserve this temporal information. As implemented in the present simulation following [222], the node index itself serves as the initial feature vector for each node when processed by the GNN, directly incorporating temporal context. The overall framework's reliability is highly sensitive to the PCD's accuracy; errors in pairwise classification (false positives or false negatives) lead to erroneous graph structures (spurious or missing edges), which can mislead the GNN and result in misclassification of the entire sequence. Therefore, achieving high PCD accuracy is critical for effective graph construction and subsequent GNN-based detection.

5.7 GNN Implementation for Spoofing Classification

The final stage of the SDR-DL detection framework utilizes a GNN specifically designed for graph-level classification. Its purpose is to analyze the entire graph $G = (V, E)$, constructed from the PCD outputs as described previously, and determine whether the underlying sequence of C-V2X messages is "legitimate" (hypothesis H_0) or "spoofed" (H_1) [222]. The GNN is trained to identify discriminative structural patterns and node feature distributions within the graph that distinguish these two classes.

The GNN takes the graph G as input, which encapsulates both connectivity information derived from PCD decisions and node specific attributes. The output is a binary classification label for the entire graph. Based on the reference work [222]

and the present simulation, the architecture involves several key components. A defining feature is the initialization of node features: the initial feature vector $h_j^{(0)}$ for each node j is simply its index in the original time-ordered sequence, $h_j^{(0)} = j$. This design choice directly encodes temporal sequence information into the GNN, allowing it to leverage both connectivity and relative message timing. The core of the GNN consists of multiple message passing layers ($L = 3$ suggested in [222], though the present simulation used $L = 2$ GCN layers effectively). In each layer l, a node j updates its representation $h_j^{(l)}$ by aggregating information from its neighbors (nodes k where $(k, j) \in E$) and combining it with its own previous representation $h_j^{(l-1)}$. While [222] describes a specific update mechanism using two DNNs per layer, standard GNN convolutional layers, such as the GCN layer [255], used in the present simulation via PyTorch Geometric's `GCNConv`, provide an effective means for neighborhood aggregation and feature transformation. The aggregation operator is typically summation [222], implicitly handled with normalization in standard GCN layers. After the final message passing layer, a graph readout function, such as global mean pooling (averaging final node features $h_j^{(L)}$ across all nodes, implemented via `global_mean_pool` in PyG), is applied to obtain a fixed size graph embedding vector. This vector summarizes the graph's structural and feature information and is fed into a final classification head, usually one or more fully connected layers (a single `Linear` layer in the present simulation) with an appropriate activation (e.g., LogSoftmax or Sigmoid), to produce the final class probabilities.

Implementing GNNs requires specialized Python libraries like PyTorch Geometric (PyG) [256] or Spektral [257]. PyG, built on PyTorch, is a leading choice offering extensive GNN layers, utilities for graph data representation (`Data` objects) and batching (`Batch`, `DataLoader`) [246, 256], and benchmark datasets. Spektral integrates with TensorFlow/Keras, providing similar functionalities [257, 258]. The choice often depends on the preferred underlying framework; the present simulation successfully used PyG.

Implementing the GNN model in PyG involves converting the NetworkX graph G into PyG's `Data` object format [256]. This requires extracting the `edge_index` (source and target nodes for edges in COO format), the node feature tensor `x` (initialized with node indices: `torch.arange(num_nodes, dtype=torch.float).view(-1, 1)`), and the graph label `y`. A PyTorch module (`SpoofingGNN` in code) is defined, encapsulating `GCNConv` layers (with activations and potentially Batch Normalization), the `global_mean_pool` operation applied using the `batch` vector from the `DataLoader`, and the final linear classification layer. The `forward` method defines the data flow through these components. The use of node indices as initial features ensures temporal information is available from the beginning.

Training the GNN requires a dataset of graphs labeled as "legitimate" or "spoofed". Generating this dataset involves creating diverse feature sequences for both scenarios (legitimate operations and various spoofing attacks), constructing the corresponding graphs using the trained PCD, labeling each graph with the ground truth, and formatting the collection for the GNN library (e.g., as a list of PyG `Data` objects). This process highlights a dependency cascade: GNN training quality depends on the realism of the initial sequences and the accuracy of the PCD used for graph construction. Errors from the PCD propagate into the graph structures, potentially hindering GNN learning. Generating sufficiently diverse data, especially for varied spoofing attacks, remains a challenge [259]. The present simulation used synthetically

generated RSSI sequences and the trained PCD.

The GNN training follows standard supervised learning for graph classification. PyG's `DataLoader` [246] handles efficient loading and batching of graph data. The training loop iterates through mini-batches, performs forward passes, computes loss (e.g., `NLLLoss` or `BCEWithLogitsLoss`), performs backpropagation, and updates model parameters using an optimizer (e.g., Adam). Performance is monitored on a validation set to detect overfitting and tune hyperparameters. Finally, the trained GNN model weights are saved (e.g., using `torch.save(model.state_dict(), PATH)`) for later use in evaluation or deployment.

5.8 System Integration and Performance Evaluation in Simulation

The PCD-GNN framework presented in this chapter represents an implemented proof of concept system validated through simulation based evaluation and documented in a peer reviewed publication [156] at IEEE International Conference on Cyber Security and Resilience (CSR) 2025. Unlike the Monte Carlo methodology identified in Chapter 3 as suitable future quantitative risk assessment (which remains proposed rather than implemented), the SDR-DL framework presented here constitutes a fully realized implementation with experimental validation results. This distinction is critical: the GNN-based spoofing detection system has been implemented, tested, and independently peer reviewed, establishing it as the thesis's primary practical contribution to V2X physical layer security.

The implementation status of this framework includes:

- **Working prototype**: Fully functional Python implementation (`cv2x_spoofing_detection.`
  integrating TensorFlow/Keras for PCD and PyTorch Geometric for GNN components.

- **Experimental validation**: Quantitative performance results (62% PCD accuracy, 94% GNN accuracy) obtained through systematic evaluation on synthetic datasets designed to emulate C-V2X RSSI characteristics.

- **Peer-reviewed publication**: Independent scientific validation through acceptance at IEEE CSR 2025, confirming methodological rigor and contribution significance to the research community.

- **Honest limitations**: Explicit acknowledgment that validation employed synthetic RSSI data rather than field-captured radio frequency measurements, with real-world deployment validation identified as essential future work.

This section presents the experimental methodology, quantitative results, and critical evaluation of the proof-of-concept implementation. To validate the proposed SDR-DL framework and assess its performance under controlled conditions, an integrated Python script (`cv2x_spoofing_detection.py`) was developed. This script simulates the complete end to end workflow, encompassing the core components detailed in the preceding sections. A modular design was employed to enhance clarity and maintainability. Key modules include data generation for synthesizing legitimate and spoofed RSSI sequences and preparing datasets for the PCD and GNN; the PCD

module using TensorFlow/Keras for DNN definition, training, and evaluation; the graph construction module utilizing the trained PCD and NetworkX to build graph representations from sequences; and the GNN module using PyTorch Geometric for GNN architecture definition, training, and evaluation. The main orchestration logic controls the simulation flow, parameter settings, component training, final evaluation, and result visualization.

The simulation implements a pipeline beginning with the generation of synthetic RSSI sequences for legitimate and spoofed scenarios, followed by the creation of labeled datasets for both the PCD (pairs) and GNN (graphs). The DNN based PCD is trained on the pair dataset, and its weights are saved. Subsequently, the trained PCD is loaded to process RSSI sequences, constructing corresponding NetworkX graphs which are then converted into PyTorch Geometric `Data` objects, crucially initializing node features with their temporal indices. The GNN model is then trained on the resulting graph dataset. Finally, the trained GNN is evaluated on a held out test set of graphs, and performance metrics along with visualizations are generated. This simulation focuses on the core PCD-GNN logic, bypassing real time SDR complexities to allow controlled evaluation based on synthetic RSSI data.

Performance evaluation of the final GNN classifier utilized standard binary classification metrics calculated on the test set predictions. These included accuracy (overall correct classifications), precision (proportion of predicted spoofs that were actual spoofs), recall (proportion of actual spoofs correctly identified), the F1-score (harmonic mean of precision and recall), and a confusion matrix visualizing True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN).

The simulation, executed with parameters defined in the script, demonstrated successful convergence for both the PCD and GNN training processes. Figure 5.6 illustrates the PCD training history, showing accuracy and loss curves. The PCD effectively learned to distinguish between RSSI pairs from the same versus different simulated contexts, achieving a final validation accuracy around 62%, reflecting the challenge of distinguishing pairs amidst simulated noise. The GNN's performance on the unseen test set is summarized in the confusion matrix (Figure 5.7) and classification report. The confusion matrix shows the GNN correctly identified 97 legitimate (TN) and 91 spoofed (TP) sequences, while misclassifying 3 legitimate as spoofed (FP) and 9 spoofed as legitimate (FN). The classification report indicated strong overall performance with Accuracy ≈ 0.94, Precision ≈ 0.97, Recall ≈ 0.91, and F1-Score ≈ 0.94. These results suggest that, even under the simulation's assumptions, the SDR-DL framework effectively detects simulated spoofing attacks based on RSSI patterns within this controlled environment.

5.9 Conclusion

This chapter has examined the development and validation of a comprehensive vulnerability monitoring framework for C-V2X PLS, addressing the fundamental limitations that persist in cryptographic only defense strategies. Throughout the investigation, it is established that while standardized authentication protocols such as IEEE 1609.2 provide essential message integrity verification, they cannot inherently prevent adversaries with compromised credentials from injecting cryptographically valid yet semantically false information into vehicular networks. This gap necessitates complementary security mechanisms that operate independently of higher layer trust

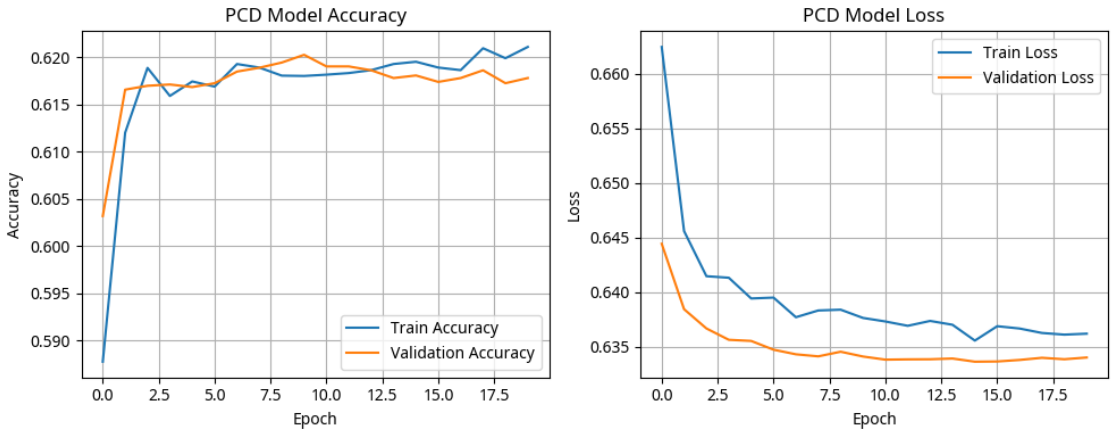


Figure 5.6: PCD Training History (Accuracy and Loss)

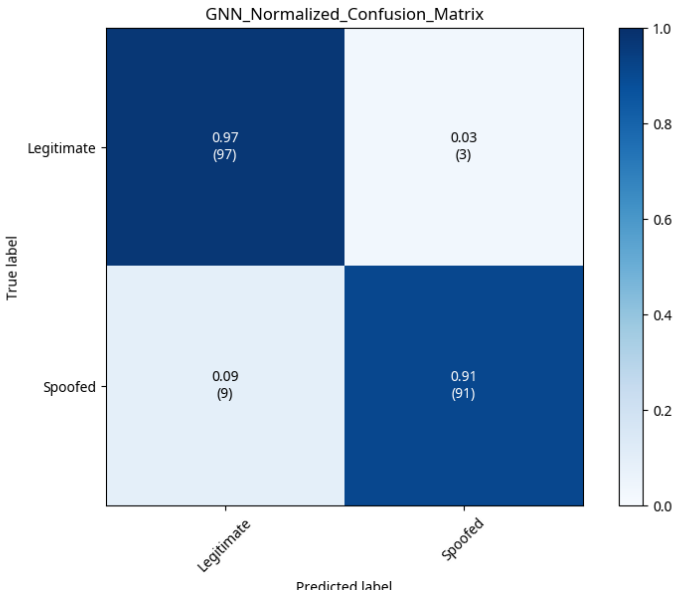


Figure 5.7: GNN Confusion Matrix on Test Set

assumptions.

The proposed SDR-DL framework integrates SDR technology with deep learning methodologies to create a two stage detection architecture specifically tailored to the dynamic characteristics of vehicular communication environments. At its foundation, the framework exploits physical layer features principally RSSI measurements extracted from raw I/Q signal samples that inherently resist manipulation due to their dependence on electromagnetic propagation phenomena including path loss, multipath fading, and Doppler effects. By capturing these features through flexible SDR platforms such as USRP hardware operating in the 5.9 GHz ITS spectrum, the system obtains access to signal characteristics that remain largely inaccessible to conventional protocol layer security implementations.

The PCD component, implemented as a deep neural network with symmetrization mechanisms to ensure order invariant classification, serves as the framework's first analytical stage. Through pairwise comparison of feature vectors extracted from messages purportedly originating from identical transmitters, the PCD identifies temporal inconsistencies that may indicate abrupt location changes characteristic of spoofing attacks. The present simulation results demonstrated that despite operating on synthetic RSSI data with inherent noise characteristics, the trained PCD achieved approximately 62% validation accuracy in distinguishing legitimate channel variations from anomalous context changes a performance level that, while modest in isolation, provides sufficient discriminatory input for subsequent graph based analysis.

The GNN stage transforms PCD outputs into structured representations where nodes correspond to temporally ordered messages and edges encode physical context consistency relationships. This architectural choice proves particularly effective because it explicitly captures the sequential nature of vehicular communications while enabling the GNN to learn discriminative patterns in graph connectivity that distinguish legitimate vehicle trajectories from spoofed message sequences. By initializing node features with temporal indices and employing GCN layers for neighborhood aggregation, the framework achieved 94% classification accuracy on simulated test data, with precision of 97% and recall of 91%. These metrics indicate that the integrated PCD-GNN architecture successfully identifies the structural signatures of spoofing attacks within controlled simulation environments.

The technical implementation revealed several critical considerations for practical deployment. First, the computational complexity of constructing graphs through exhaustive pairwise PCD evaluations scales quadratically with sequence length ($O(J^2)$), presenting significant challenges for real time processing in dense vehicular networks where message rates can reach thousands per second. Optimization strategies such as temporal windowing offer potential mitigation by restricting comparisons to messages within bounded time intervals, though this approach may compromise detection of sophisticated attacks involving non consecutive message manipulation. Second, the framework's reliance on RSSI as its primary discriminatory feature introduces vulnerability to environmental variability fast fading can induce 20-30 dB fluctuations even for stationary transmitters, requiring robust ML models capable of distinguishing natural channel variations from malicious anomalies. Third, the deep learning components inherent in both PCD and GNN stages exhibit the opacity characteristic of neural network architectures, complicating explainability requirements in safety critical vehicular applications where security decisions must be transparent and accountable.

Validation through the Python based simulation prototype (`cv2x_spoofing_detection.py`) successfully demonstrated end to end integration of SDR signal processing emulation, DNN based pairwise analysis, NetworkX graph construction, and PyTorch Geometric GNN classification. However, the simulation necessarily operated under idealized assumptions particularly regarding synthetic RSSI generation via Gaussian models and the absence of complex real world propagation effects such as non line of sight conditions, interference from heterogeneous wireless systems, and vehicle density variations. Synthetic data lack the richness of authentic C-V2X captures that would include diverse mobility patterns, varied levels of sophistication of attacks, and environmental complexity that span urban canyon scenarios, road conditions, and rural settings.

Despite these simulation constraints, the chapter establishes that PLS approaches grounded in ML analysis of SDR captured features represent a viable complement to cryptographic vehicular network defenses. The framework's ability to detect spoofing attacks through temporal consistency analysis of radio frequency characteristics provides a security layer that operates independently of certificate validity and message authentication codes. When integrated with conventional security protocols, edge computing resources, and potentially multi modal sensor fusion from GPS, inertial measurement units, and infrastructure based observations, such physical layer techniques contribute to defense in depth architectures capable of withstanding sophisticated adversaries that compromise individual security mechanisms. The quantitative performance achieved in simulation particularly the 94% accuracy with high precision suggests that with further refinement addressing real world data diversity, computational optimization, and model interpretability, SDR-DL frameworks can advance toward operational deployment in production C-V2X networks where physical layer vulnerability monitoring enhances overall vehicular cybersecurity posture.

Chapter 6

Cybersecurity Awareness Research and Training in V2X Sector

The preceding chapters of this thesis have established the technical foundations for secure V2X communications through simulation, emulation, and industrial testbed validation. These contributions address the technological dimension of V2X cybersecurity protocol design, vulnerability assessment methodologies, and defensive mechanisms. However, the successful deployment of secure V2X systems requires more than technical solutions alone. As contemporary cybersecurity incidents continue to demonstrate, the human factor represents a critical vulnerability that no amount of cryptographic sophistication or intrusion detection can fully mitigate.

This chapter bridges the gap between technical security validation and organizational security competence. It examines how testbed-based research platforms, exemplified by the CyberVehiCare testbed developed in collaboration between the University of Wolverhampton and the University of Genoa, can serve a dual purpose: not only as research instruments for vulnerability discovery but also as educational platforms for cybersecurity training. The analysis proceeds from the premise that comprehensive V2X security requires both robust technical defenses and a workforce equipped with the knowledge and skills to implement, maintain, and continuously improve these defenses.
[1]

6.1 Introduction to Cybersecurity Awareness in Automotive V2X Systems

6.1.1 The Paradigm Shift: From Mechanical Safety to Cyber-Physical Security

The automotive industry has undergone a fundamental transformation over the past two decades, evolving from a domain dominated by mechanical engineering principles to a complex cyber physical ecosystem where software and connectivity

[1]The content of this Chapter has been published in the following papers and patent:
M. A. Rahman et al., "CyberVehiCare: A Testbed for Cybersecurity of Vehicle to Everything (V2X) Automotive Systems," 2025 IEEE International Conference on Cyber Security and Resilience (CSR), Chania, Crete, Greece, 2025, pp. 818-823, doi: 10.1109/CSR64739.2025.11130024.

play increasingly critical roles. This evolution presents a profound paradox: the same technologies that enhance vehicle safety through cooperative sensing and real time information sharing also introduce unprecedented attack surfaces that threaten the very safety they aim to improve.

In the year 2000, a typical passenger vehicle contained approximately 30 ECUs managing discrete functions, such as engine management, anti lock braking, and basic climate control. By 2010, luxury vehicles incorporated more than 100 ECUs, interconnected through CAN bus [28] and LIN bus [29]. The introduction of V2X communication technologies, encompassing V2V, V2I, V2P, and V2N modalities, has extended the vehicle's electronic architecture beyond its physical boundaries, creating a distributed system vulnerable to remote attacks.

The Society of Automotive Engineers (SAE) taxonomy of driving automation [260] defines six levels of autonomy (Levels 0–5), with higher automation levels requiring increasingly sophisticated sensing, communication, and decision making capabilities. As vehicles progress toward SAE Levels 4 and 5, their dependence on external data sources, including V2X communications, correspondingly intensifies. A vehicle operating at Level 4 autonomy relies on V2X messages, such as BSMs, CAMs, and DENMs, to augment onboard sensor data and make safety critical decisions. The compromise of these communication channels through jamming, message injection, or spoofing attacks could directly undermine the vehicle's safety functions.

The 2013 demonstration by Miller and Valasek [261], in which researchers achieved remote control of a Jeep Cherokee's critical systems through exploitation of its cellular connectivity and CAN bus architecture, served as a watershed moment for the automotive cybersecurity community. This incident illustrated that vehicular systems, historically protected by isolation and obscurity, had become accessible to sophisticated attackers. Figure 6.1 shows Automotive cybersecurity evolution timeline from 2000 to 2024, highlighting key milestones including early connectivity (30 ECUs in 2000), the Miller & Valasek Jeep Cherokee remote hack (2013), V2X deployment (2016), and the introduction of regulatory frameworks ISO/SAE 21434 [138] and UN R155 [139] (2021). The research revealed fundamental vulnerabilities stemming from the automotive industry's traditional engineering culture, which had not adequately integrated security-by-design principles developed in the information technology domain.

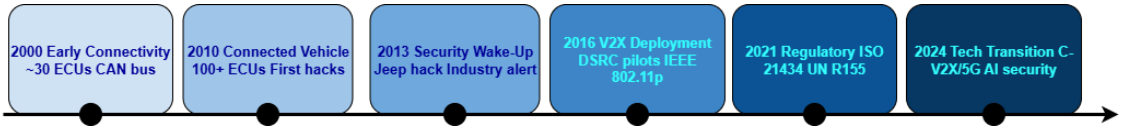


Figure 6.1: Automotive cybersecurity evolution timeline.

V2X communication systems introduce wireless attack surfaces that fundamentally differ from in vehicle network vulnerabilities. The DSRC standard, based on IEEE 802.11p operating in the 5.9 GHz ITS band, employs OFDM to enable low-latency message exchange within a range of approximately 300–500 meters. While IEEE 1609.2 defines security services including message authentication and confidentiality through Public Key Infrastructure (PKI) and ECDSA, the protocol's real time performance requirements BSM transmission every 100 ms with end-to-end latency below 100 ms constrain the computational resources available for security processing [10]. This tension between performance and security creates opportunities for attacks

that exploit timing vulnerabilities or resource exhaustion. Figure 6.2 shows the V2X attack surface taxonomy organized into four main categories: in-vehicle networks (CAN/LIN bus vulnerabilities, ECU firmware exploits, OBD-II physical access), wireless communications (DSRC/C-V2X RF jamming, message injection, MAC spoofing), external services (GPS spoofing, cellular MitM), and cloud backend (PKI compromise, malicious firmware updates). Color coding indicates threat severity.

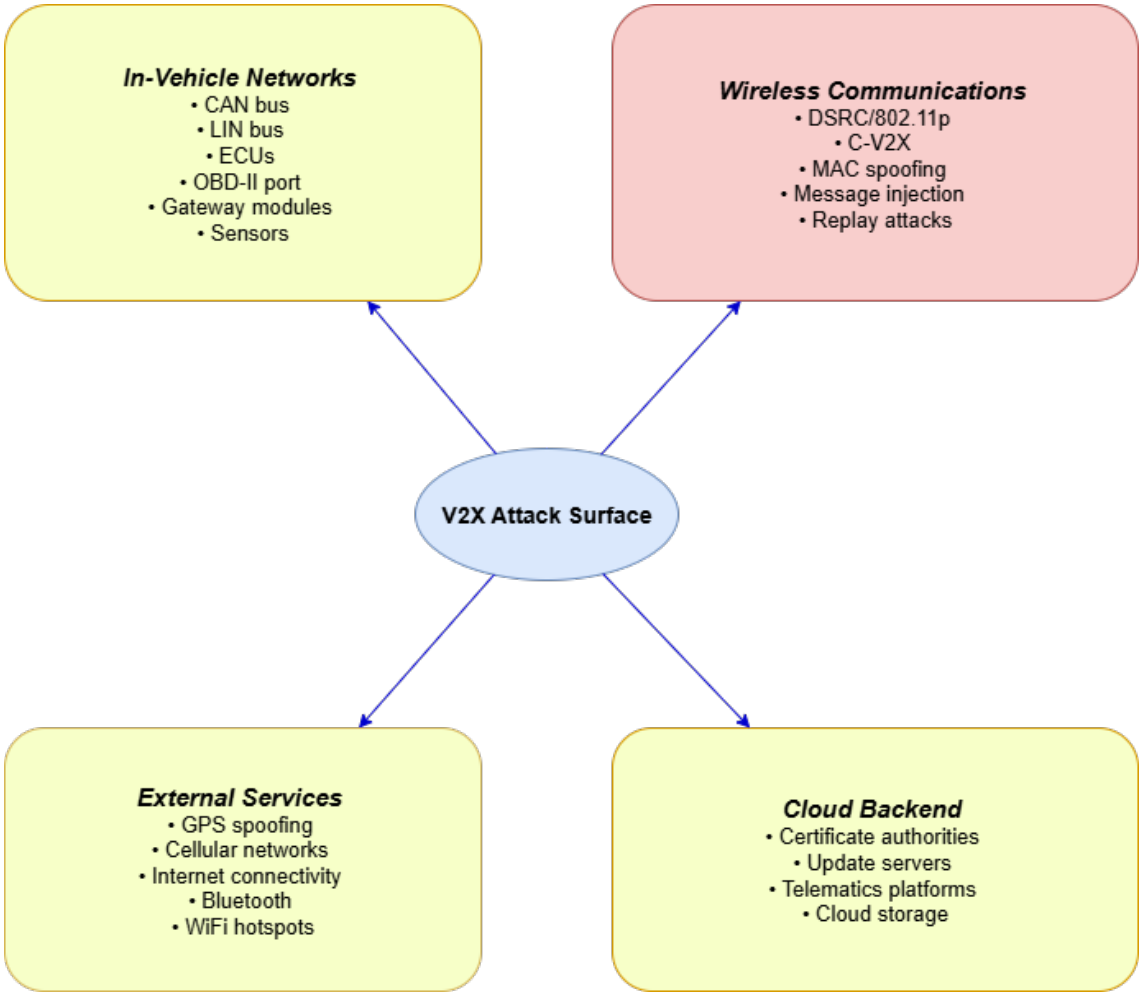


Figure 6.2: V2X attack surface taxonomy.

The parallel emergence of C-V2X, standardized by the 3GPP as part of LTE Release 14 and subsequent 5G New Radio releases, introduces additional security considerations related to cellular network infrastructure, spectrum licensing, and coexistence with DSRC deployments [50, 262]. The industry faces a critical decision point regarding V2X technology adoption, with different regions pursuing divergent strategies: the United States has reallocated portions of the 5.9 GHz band away from DSRC toward unlicensed use, while Europe and Asia continue to evaluate both technologies. This technological uncertainty complicates cybersecurity training initiatives, which must prepare practitioners for multiple potential deployment scenarios.

6.1.2 The Human Factor: Why Technical Solutions Are Not Sufficient

Cybersecurity is fundamentally a socio technical challenge that cannot be resolved through technological measures alone. Empirical analysis of cybersecurity incidents across industries consistently identifies human, such as inadequate training, misconfiguration, social engineering, and insider threats, as contributing factors in 40–60% of successful attacks. The automotive domain, with its complex supply chains, distributed development processes, and traditional engineering culture not historically focused on security, faces particular challenges in establishing organizational cybersecurity competence.

The ISO/SAE 21434:2021 standard "Road vehicles Cybersecurity engineering" represents the automotive industry's comprehensive response to cybersecurity risks throughout the vehicle lifecycle [138]. Clause 5 "Organizational cybersecurity management" explicitly addresses the human dimension through requirements for cybersecurity culture, governance, and competence. Clause 5.4.2 mandates that: "The organization shall ensure that personnel have adequate cybersecurity awareness and competence for performing their assigned cybersecurity activities". This regulatory requirement establishes cybersecurity training not as an optional enhancement but as a mandatory prerequisite for compliance with automotive cybersecurity standards.

The UN Regulation No. 155 (UN R155) "Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system" further reinforces these requirements through binding regulations applicable to vehicles sold in UNECE member states [139]. Annex 5, Part A, requires manufacturers to implement "training and awareness programs" as components of their CSMS. The regulation's enforcement mechanism vehicles without approved CSMS cannot be type approved for sale, providing strong incentives for manufacturers to invest in workforce cybersecurity competence development. However, meeting these regulatory requirements presents significant practical challenges. Automotive engineers typically possess deep expertise in mechanical systems, electrical engineering, or embedded software development, but relatively few have received formal education in cybersecurity principles, threat modeling, or secure development practices. The skill requirements for V2X security span multiple technical domains: RF engineering (understanding DSRC/C-V2X physical layer vulnerabilities) [157, 263], network protocol analysis (IEEE 1609 family of standards, 3GPP specifications), cryptography (PKI, ECDSA, hash functions) [91], and wireless security (jamming, eavesdropping, man in the middle attacks) [182, 264]. This interdisciplinary nature creates a significant competence gap that traditional university curricula and corporate training programs have struggled to address.

The automotive supply chain's complexity further complicates competence development efforts. Modern vehicles integrate components from hundreds of Tier-1, Tier-2, and Tier-3 suppliers, each with varying levels of cybersecurity maturity. The requirements of ISO/SAE 21434, Clause 5, apply throughout the supply chain, necessitating coordinated training initiatives that extend beyond Original Equipment Manufacturers (OEMs) to encompass the entire automotive ecosystem [138]. The National Highway Traffic Safety Administration's (NHTSA) "Cybersecurity Best Practices for the Safety of Modern Vehicles" identifies workforce development and continuous education as crucial steps for improving automotive cybersecurity, recog-

nizing that technical controls alone cannot substitute for organizational competence [265].

6.1.3 Chapter Scope and Research Questions

This chapter addresses a critical research gap at the intersection of V2X cybersecurity technology and workforce development. While substantial academic literature exists on V2X protocol security, vulnerability assessment methodologies, and defensive mechanisms, considerably less attention has been devoted to the systemetic translation of how security knowledge generated through research activities. The testbed based approach, in which researchers develop physical or hybrid platforms integrating real automotive components with emulated communication systems, offers particular promise for dual purpose utilization as both research instruments and training environments.

This chapter demonstrates that testbed based research platforms serve a dual purpose for both technical security validation and educational cybersecurity training in the V2X domain. This demonstration addresses four key aspects:

1. Competency frameworks applicable to V2X cybersecurity workforce deployment are identified and aligned with regulatory requirements including ISO/SAE 21434 and UN R155.

2. Research findings from testbed based vulnerability assessment are systematically transformed into educational training modules through structured knowledge translation processes.

3. Organizational processes that translate cybersecurity awareness and training initiatives into measurable risk mitigation in production V2X deployments are examined and validated.

4. Evaluation metrics assess the effectiveness of cybersecurity training programs in achieving regulatory compliance and reducing security vulnerabilities.

The chapter describes the CyberVehiCare testbed [266], developed in cooperation with the University of Wolverhampton, as a primary case study. CyberVehiCare integrates authentic automotive components, including ECUs, climate control systems, instrument clusters, and CAN/LIN network infrastructure, with SDR platforms for V2X communication emulation. The testbed's design explicitly accommodates research applications (vulnerability discovery, attack validation, defense mechanism testing) and educational applications (hands-on cybersecurity training, competency assessment, curriculum development).

This chapter's position within the broader thesis reflects its complementary relationship with the preceding technical chapters. Chapters 3, 4 and 5 establish methodologies for V2X security analysis through simulation, emulation, and testbed validation, generating technical knowledge about protocol vulnerabilities, attack feasibility, and defense effectiveness. This Chapter extends the technical foundation by examining how this knowledge can be operationalized into organizational competence, thus addressing the complete life cycle from research discovery to practitioner

implementation. This integration of technical and human factors aligns with contemporary cybersecurity frameworks that recognize security as an emerging property of socio technical systems rather than a purely technological attribute.

The chapter proceeds as follows. Section 6.2 surveys the current state of cyber ranges, testbeds, and training methodologies, establishing the broader context for automotive cybersecurity education. Section 6.3 presents a detailed examination of the CyberVehiCare testbed's architecture and training capabilities, demonstrating how research platforms can support educational objectives. Section 6.6 proposes a three tier competency model (Awareness, Training, Education) and describes organizational processes for translating testbed-derived knowledge into workforce competence. Section 6.7 identifies current limitations and discusses emerging solutions, including cloud-based cyber ranges, digital twins, and automated vulnerability discovery. Section 6.8 synthesizes the contribution of the chapter and its implications for both research and practice.

6.2 Research Landscape: Cybersecurity Training Methodologies for V2X

6.2.1 Cyber Ranges and Testbeds: Taxonomy and Evolution

Cyber ranges and cybersecurity testbeds represent essential infrastructure for security research, training, and operational exercises. These platforms provide controlled environments where security professionals can develop and validate attack techniques, test defensive mechanisms, and practice incident response without risking production systems or violating legal constraints. While historically distinct in their primary purposes cyber ranges emphasizing training and exercises, testbeds focusing on research and technology validation, recent years have witnessed increasing convergence of these platform types in terms of capabilities and applications. Yamin et al. provide a comprehensive taxonomy of cyber range systems based on extensive literature analysis [267]. Their framework classifies cyber ranges along multiple dimensions, including architecture (physical, virtualized, hybrid), scenario design (attack-defense, capture-the-flag, red team-blue team), and primary application domain (academic, government, military, commercial). This taxonomy reveals significant diversity in cyber range implementations, reflecting the varied objectives and constraints of different user communities. Chouliaras et al. surveyed ten prominent cyber ranges developed over the past decade, analyzing their design principles, technological foundations, and educational methodologies [268]. Their analysis identifies common architectural elements including virtualization platforms (VMware, KVM, Xen), container orchestration systems (Docker, Kubernetes), and network simulation tools (GNS3, EVE-NG). These technological building blocks enable rapid deployment of complex network topologies, automated scenario generation, and scalable multi-user training exercises. Ukwandu et al. conducted a more extensive review encompassing 24 testbed and cyber range platforms from 2010 to 2020, providing a historical perspective on the evolution of these systems [269]. Their analysis reveals increasing convergence between cyber ranges and testbeds, with platforms originally designed for research applications progressively incorporating training capabilities, and training-focused ranges adopting research-oriented features, such as data collection and

experimental reproducibility. This convergence reflects growing recognition that the boundary between research and training represents an artificial distinction: effective training requires access to realistic attack scenarios derived from research, while meaningful research benefits from practitioner feedback obtained through training exercises. Table 6.1 categorizes cyber ranges according to their primary organizational context and applicability to V2X automotive cybersecurity.

Table 6.1: Cyber Range Taxonomy for V2X Training

Category	**Primary Purpose**	**Typical Users**	**V2X Relevance**
Academic	Research + Education	Users, Researchers	Medium
Government	Policy + Workforce Development	NIST, NHTSA, ENISA	High
Military	Defense + Critical Infrastructure	DoD, NATO	Low
Commercial	Product Testing + Certifications	OEMs, Tier-1 Suppliers	Very High

The V2X relevance assessment in Table 6.1 reflects several domain specific considerations. Academic cyber ranges possess medium relevance due to their flexibility and experimental nature, enabling exploration of emerging V2X technologies without the constraints of production systems. However, academic platforms often lack authentic automotive components and may not adequately replicate the resource constraints, real time requirements, and safety implications characteristic of vehicular systems.

Government cyber ranges demonstrate high relevance for V2X applications. Organizations such as the National Highway Traffic Safety Administration (NHTSA) in the United States and the European Union Agency for Cybersecurity (ENISA) have developed specific initiatives addressing vehicle cybersecurity, including training curriculum development and workforce competency frameworks [270, 271]. The NHTSA's program of Vehicle Cybersecurity Training Curriculum Pilot Testing, conducted in collaboration with the Automotive Information Sharing and Analysis Center (Auto-ISAC) [272], exemplifies government investment in developing standardized training approaches that can be adopted in the automotive industry.

Military cyber ranges exhibit lower V2X relevance despite their technical sophistication. Although military applications increasingly involve connected vehicle technologies, particularly in the context of autonomous military vehicles and convoy operations, the specialized requirements of military systems (including classified technologies, adversarial threat models, and operational security constraints) limit direct applicability to civilian automotive contexts.

Commercial cyber ranges represent the category with the highest V2X relevance. Original equipment manufacturers and Tier-1 automotive suppliers require platforms that incorporate authentic vehicle components, replicate production network architectures, and support compliance testing against standards, such as ISO/SAE 21434 and UN R155 [138, 139]. Commercial platforms must balance realism, using actual ECUs, communication protocols, and vehicle systems, with safety, preventing destructive attacks that could damage expensive hardware, and scalability, supporting training for large engineering workforces.

Pospisil et al. examined cybersecurity testbeds specifically for Industrial Control Systems (ICS), identifying design principles that partially transfer to automotive applications [273]. Both ICS and automotive systems share characteristics including real time constraints, safety critical operations, long operational lifetimes, and legacy components lacking modern security features. Their analysis emphasizes the importance of Hardware in the Loop (HIL) capabilities, which enable testing of actual control algorithms and network protocols under realistic timing and resource constraints. This HIL approach proves particularly valuable for V2X systems where message latency directly impacts safety a 100 ms delay in BSM delivery could result in a vehicle failing to detect an imminent collision.

6.2.2 Automotive Cybersecurity Testbeds: State of the Art

The automotive cybersecurity research community has developed numerous testbed platforms over the past 15 years, reflecting the growing recognition of vehicular systems as critical cybersecurity domains. Mahmood et al. conducted a comprehensive survey of automotive cybersecurity testing methodologies, analyzing seven prominent testbeds developed between 2010 and 2020 [274]. Their analysis identifies four primary testing methodologies: vulnerability scanning (automated detection of known weakness patterns), penetration testing (manual exploitation of vulnerabilities to assess exploitability), fuzzing (generation of malformed inputs to trigger unexpected behavior), and HIL validation (testing with actual vehicle components under controlled conditions).

The main developed automotive cybersecurity testbeds are:

- **HybridgeCAN** [275]: developed by Granata et al., represents a hybrid testbed architecture that bridges physical and virtual CAN bus segments. The platform enables researchers to inject real CAN bus traffic into simulated network segments, facilitating large-scale experiments that would be impractical with purely physical implementations. HybridgeCAN supports both attack emulation (injection of malicious CAN frames) and defense validation (testing of intrusion detection systems and gateway filtering rules). However, the platform's focus on vehicle network security means but it lacks comprehensive V2X communication capabilities, limiting its applicability for training on wireless attack vectors, such as RF jamming, MAC layer spoofing, and Over-the-Air (OTA) message manipulation.

- **Open Car Testbed and Network Experiments (OCTANE)** [276]: introduced by Everett and McCoy in 2013, pioneered the concept of vendor-neutral automotive cybersecurity research platforms. OCTANE combines software packages for CAN bus simulation and analysis with a hardware framework that supports connection of various types of ECU. The platform's educational orientation makes it particularly relevant for academic institutions, providing users with hands-on experience in automotive network architectures and attack techniques. However, OCTANE's age represents a limitation, as the platform predates widespread V2X deployment and consequently lacks dedicated support for DSRC or C-V2X protocols. The testbed's architecture could potentially be extended to incorporate V2X capabilities through the addition of wireless communication modules and SDR platforms.

- **Portable Automotive Security Testbed with Adaptability (PASTA)** [277]: presented by Toyama et al. at Black Hat Europe 2018, addresses the portability challenge that limits many automotive testbeds. Traditional testbeds often require dedicated laboratory space and permanent installation, constraining their accessibility for training purposes. PASTA employs custom designed white box ECUs with documented architectures and open-source firmware—enabling vendor-independent security research. This design choice proves particularly valuable for training applications, as users can examine ECU internals, modify firmware, and experiment with attack techniques without restrictions imposed by proprietary systems. White box ECUs sacrifice some realism compared to commercial automotive components, but provide pedagogical advantages through complete transparency. PASTA has achieved recognition as one of the most advanced portable automotive security testbeds currently available, demonstrating capabilities including engine control manipulation, brake system testing, and infotainment system exploitation. However, even PASTA's comprehensive feature set does not fully encompass V2X external communication testing. The testbed's current iteration focuses primarily on in-vehicle network security and ECU vulnerabilities, representing the more mature subdomain of automotive cybersecurity research. The relative immaturity of V2X cybersecurity testbeds reflects both the technology's recent emergence and the technical complexity of replicating wireless communication environments with adequate fidelity.

- **Security Portable Automotive Testbed (SPAT)** [278]: developed by Caviglia et al. at the University of Genova, represents more recent work explicitly oriented toward cybersecurity training. SPAT's initial prototype demonstrates fundamental vehicle functions including controls for mechanical movement (steering, acceleration, braking) and auxiliary systems (lighting, climate control). The testbed architecture supports progressive complexity scaling, starting with basic CAN bus communication and advancing to more sophisticated attack scenarios. SPAT's design philosophy emphasizes educational accessibility, with documentation and training materials developed concurrently with the hardware platform. However, the authors acknowledge that the V2X capabilities remain incompletely investigated in SPAT's current implementation, representing a priority for future development.

- **CyberVehiCare** [266]: developed at the University of Wolverhampton, is the only platform in this analysis that offers comprehensive V2X communication capabilities through SDR integration along with CAN/LIN bus. This distinctive feature highlights the testbed's design objective of extending security research beyond in-vehicle networks to encompass external vehicular communications. The testbed integrates multiple cybersecurity protection mechanisms to mitigate diverse attack vectors across different subsystems. For the in-vehicle CAN bus, a gateway control module (1K0907530S) filters malicious frames, and the OBD interface employs Transport Layer Security (TLS) 1.3 to ensure secure data exchanges. Wireless interfaces are protected by a 500 m signal threshold–based jamming detection system and MAC address whitelisting configured in the Wi-Fi network layer. Sensor subsystems implement advanced cryptographic protections: temperature sensor data (3D0907543A) are digitally signed using

the ECDSA, while brake fluid level sensor readings (1K2611349A) are secured using Secure Hash Algorithm 256 (SHA-256) hashing.

Table 6.2 provides a comparison among these automotive testbeds highlighting V2X support, CAN bus testing, portability, SDR integration, training focus, and use of real vehicle components. This comparison highlights CyberVehiCare's uniqueness among all other testbeds, as it supports the most comprehensive set of features.

Table 6.2: Automotive Testbed Feature Comparison

Testbed	**V2X**	**CAN**	**Port.**	**SDR**	**Train.**	**Real**
HybridgeCAN	✗	✓	❒	✗	❒	❒
OCTANE	✗	✓	✓	✗	✓	✗
PASTA	✗	✓	✓	✗	✓	❒
SPAT	❒	✓	✓	✗	✓	✓
CyberVehiCare	✓	✓	❒	✓	✓	✓

Legend: ✓ = Feature fully supported; ❒ = Partial support; ✗ = Not supported

6.2.3 V2X Specific Training Requirements and Challenges

V2X communication security introduces qualitatively distinct challenges from in-vehicle network security, necessitating specialized training approaches that conventional automotive cybersecurity curricula may not adequately address. These unique requirements emerge from the fundamental characteristics of wireless vehicular communications, including RF propagation, mobility dynamics, real time latency constraints, and safety critical message semantics.

Wireless Attack Surface. Unlike CAN bus security, which primarily concerns adversaries with physical access to the vehicle or its diagnostic port, V2X security must account for wireless attackers potentially located hundreds of meters from their targets. The DSRC operating range of 300–500 meters means that any person near a highway can potentially observe, jam, or inject V2X messages. This attack surface expansion transforms vehicle security from a relatively contained problem (requiring physical access) to a broadcast problem (accessible to any nearby adversary).

Training for wireless security requires competencies in several technical domains. RF engineering knowledge enables understanding of physical layer vulnerabilities including jamming (intentional interference preventing legitimate communications), eavesdropping (passive observation of cleartext or weakly encrypted messages), and signal manipulation (RF fingerprinting, replay attacks). The IEEE 802.11p physical layer [8] employs OFDM modulation with 10 MHz channel bandwidth, operating at half the symbol rate of conventional 802.11a WiFi to accommodate Doppler shifts from vehicle motion. Security practitioners must understand how these physical layer characteristics affect attack feasibility and detection strategies [193].

Real Time Constraints. V2X protocols prioritize low latency to support safety critical applications. SAE J2735 specifies that vehicles should transmit BSMs every 100 ms, containing position, velocity, acceleration, and vehicle state information [11]. The IEEE 1609.3 networking services standard defines QoS requirements for message delivery, with different priorities for safety critical, traffic efficiency, and infotainment applications [11].

These timing requirements constrain the computational resources available for security operations. PKI operations, including certificate validation and ECDSA signature verification[85, 154, 155], consume valuable processor cycles that must be budgeted against real time message processing requirements [91]. Training programs must therefore address not only security mechanism design but also performance optimization and resource management under real time constraints, skills rarely emphasized in conventional cybersecurity curricula focused on enterprise IT systems without strict latency requirements.

Protocol Stack Complexity. The V2X protocol stack consists of multiple standardized layers, each exposing distinct security vulnerabilities. The physical layer, defined by IEEE 802.11p and 3GPP LTE/5G-V2X specifications, governs the characteristics of radio transmission. The data link layer includes MAC defined in IEEE 802.11p and the Logical Link Control sublayer [8]. To enable efficient spectrum utilization, IEEE 1609.4 specifies multi-channel operations, allowing vehicles to alternate between control channels for safety critical messaging and service channels for non safety applications [12].

As shown in Figure 6.3, the V2X attack layer taxonomy maps threats to OSI style layers. Physical layer attacks, such as RF jamming and eavesdropping are the hardest to detect, while data link and network layer attacks (e.g., MAC spoofing, replay, routing manipulation, DoS) exhibit moderate detection difficulty. Application layer attacks, including message injection and certificate forgery, are comparatively easier to identify due to the cryptographic validation mechanisms defined in IEEE 1609.2 [10].

IEEE 1609.2 [10] defines security services operating across multiple layers, including message authentication through ECDSA-based signatures [85, 154, 155], confidentiality through encryption, and trust management through certificate hierarchies. The most recent version (IEEE 1609.2-2022 [77]) refines these mechanisms based on deployment experience. Training programs must develop competence not only in individual protocol layers but in understanding cross layer interactions and attack vectors that exploit inconsistencies between layers.

Regulatory Training Mandates. ISO/SAE 21434 Clause 5.4.2 mandates that organizations "ensure personnel have adequate cybersecurity awareness and competence for performing their assigned cybersecurity activities" [138]. This requirement applies throughout the automotive supply chain, from OEMs to semiconductor suppliers. Clause 6.4.3 further specifies that cybersecurity engineering activities shall be performed by personnel with demonstrated competence, requiring organizations to establish competence criteria and verification mechanisms.

UN R155, Annex 5 Part A, requires cybersecurity management systems to include "training and awareness programs" without specifying detailed requirements regarding duration, content, or assessment methods [139]. This regulatory ambiguity creates challenges for organizations seeking to demonstrate compliance, as the standard's performance based approach (specifying objectives rather than prescriptive requirements) necessitates professional judgment in determining what constitutes "adequate" training.

The Automotive Information Sharing and Analysis Center (Auto-ISAC) Automotive Cybersecurity Training (ACT) Program represents an industry response to this regulatory gap [158]. The ACT Program provides a comprehensive curriculum addressing cybersecurity throughout the vehicle lifecycle, with modules covering

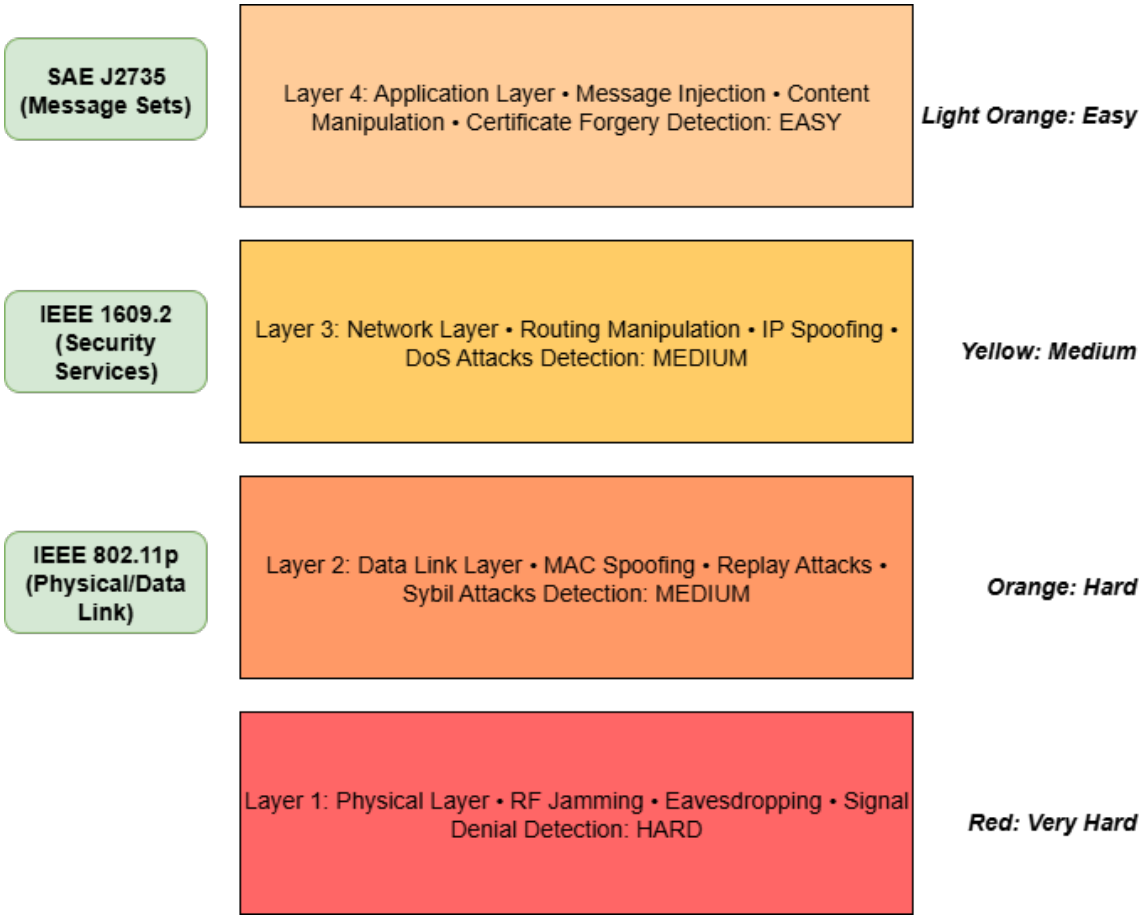


Figure 6.3: V2X attack layer taxonomy mapping threats.

threat modeling, secure development practices, vulnerability management, and incident response. Training completion satisfies the UN R155 requirement for formal cybersecurity training, providing a standardized baseline that organizations can adopt to demonstrate regulatory compliance.

The ENISA has published extensive guidance on smart car cybersecurity [279, 280], identifying good practices organized into three categories: policy and standards, organizational measures, and security functions. The organizational measures category explicitly addresses training and awareness, recommending that automotive organizations establish formal competency frameworks, conduct regular skills assessments, and maintain training records demonstrating ongoing professional development.

These regulatory and policy frameworks establish cybersecurity training not as an optional best practice but as a mandatory compliance requirement. However, they also reveal a significant implementation challenge: while regulations mandate training, they provide limited guidance on pedagogical approaches, competency assessment methods, or training effectiveness metrics. This creates an opportunity for testbed based training platforms to provide concrete, measurable, and verifiable approaches to competence development.

6.3 CyberVehiCare: A Case Study in Research-Driven Cybersecurity Training

The CyberVehiCare testbed, developed at the University of Wolverhampton, exemplifies the dual purpose design philosophy, whereby a research platform for cybersecurity validation simultaneously serves as an educational environment for training. This section examines CyberVehiCare's architecture, training capabilities, and empirical validation results, demonstrating how testbed based approaches can systematically translate research findings into practitioner competence. Figure 6.4 presents a photograph of the CyberVehiCare testbed, while Figure 6.5 illustrates its architectural framework.



Figure 6.4: CyberVehiCare prototype testbed Architecture.

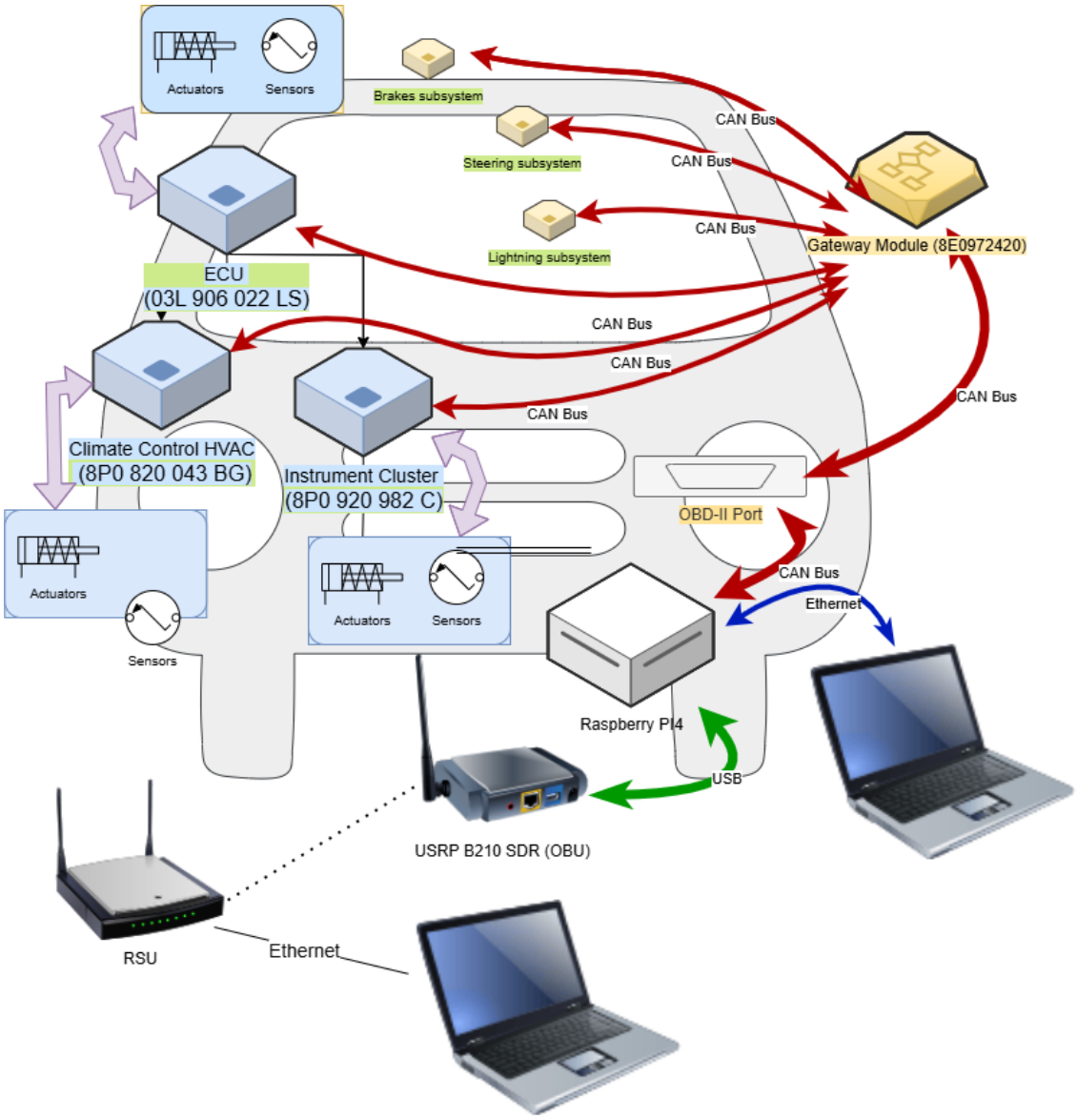


Figure 6.5: Block diagram of the testbed.

6.3.1 Testbed Architecture and Dual Purpose Design

CyberVehiCare [266] integrates authentic automotive components with emulated V2X communication modules, achieving a balance between realism (using actual vehicle hardware) and safety (preventing destructive attacks on expensive equipment). The testbed's architecture encompasses three primary subsystems: in-vehicle networks and components, V2X communication infrastructure, and monitoring and control systems.

In-Vehicle Systems. The testbed incorporates production automotive components extracted from commercial vehicles, providing authentic electrical characteristics, timing behaviors, and protocol implementations. The engine and powertrain subsystem includes an engine control unit (ECU model 03L906022LS) with supporting peripherals including a fuel pump (1K0906089A), turbocharger actuator (03L198716A), and multiple sensors monitoring exhaust temperature (03L906088N CC) and air flow (03G906461C). These components communicate via CAN bus,

exchanging messages related to engine management, emissions control, and diagnostic functions.

The climate control subsystem features an HVAC module (8P0820043BG) with associated temperature sensors (4B0820539), air quality detectors (4B0907659A), and motorized flaps (1K2907511E) that regulate cabin conditions. Vehicle control and safety components include lighting circuits with headlight connectors and hazard switches (8P0941509D), steering components with angle sensors (1K0959654) and ignition switches (1K0905851), and braking system sensors that monitor fluid levels (1K2611349A) and pad wear indicators.

The instrument cluster (8P0920982C) and the immobilizer provide targets to examine attacks against driver information displays and anti theft systems. Training scenarios might involve spoofing speed readings displayed to the driver or attempting to bypass ignition security, with corresponding defensive strategies including encrypted cluster communications and multi factor authentication for vehicle start up. Figures 6.5 and 6.6 illustrate invehicle systems (engine/powertrain ECU, climate control HVAC, vehicle control components, instrument cluster) interconnected via CAN/LIN buses through a gateway control module, with V2X communication infrastructure comprising Raspberry-Pi-4 middleware, SDR platforms (bladeRF 2.0 OBU, USRP B210 RSU), and six training modules targeting specific attack surfaces.

The network infrastructure comprises CAN and LIN buses connecting these critical components, with an OBD-II diagnostic port (3A0972695 connector) serving as a primary access point for both legitimate diagnostic tools and potential attack vectors. A gateway control module (8E0972420) manages message routing between different CAN bus segments, implementing filtering rules intended to prevent malicious message propagation.

V2X Communication Infrastructure. CyberVehiCare's distinguishing feature relative to existing automotive testbeds is its comprehensive V2X communication capability implemented through SDR platforms. The testbed deploys separate SDR configurations for OBU and RSU functionality, enabling realistic emulation of vehicle to infrastructure communications. The OBU implementation employs a Raspberry Pi-4 single board computer as middleware, interfacing between the vehicle's internal networks and external V2X communications. A Nuand bladeRF 2.0 micro xA4 SDR (operational frequency range 47 MHz to 6 GHz, maximum sampling rate 61.44 MHz) connects to the Raspberry Pi via USB 3.0. The receiver configuration operates at 5.80 GHz center frequency with 40 dB RF gain, providing 95 dBm sensitivity for robust signal reception. A 64 point FFT implements OFDM demodulation and frame equalization. The OBU's tri-band antenna covers frequencies between 700 MHz and 2.6 GHz, accommodating DSRC communications experimentation. To enhance interoperability and real-time vehicular interfacing, the OBU integrates a Vector VN4610 module, which provides 802.11p, CAN (FD), and GNSS connectivity. The VN4610 acts as a bridge between the SDR-based OBU and the in-vehicle network, enabling synchronized data exchange across RF, CAN, and positioning layers. This allows precise timestamping, message correlation, and validation of communication events under realistic driving conditions. The VN4610 also facilitates time-aligned GNSS-based synchronization, ensuring that transmitted and received frames adhere to the strict temporal requirements of V2X protocols. Together, the integration of the bladeRF SDR and the Vector VN4610 module establishes a comprehensive experimental framework for both functional and security-oriented

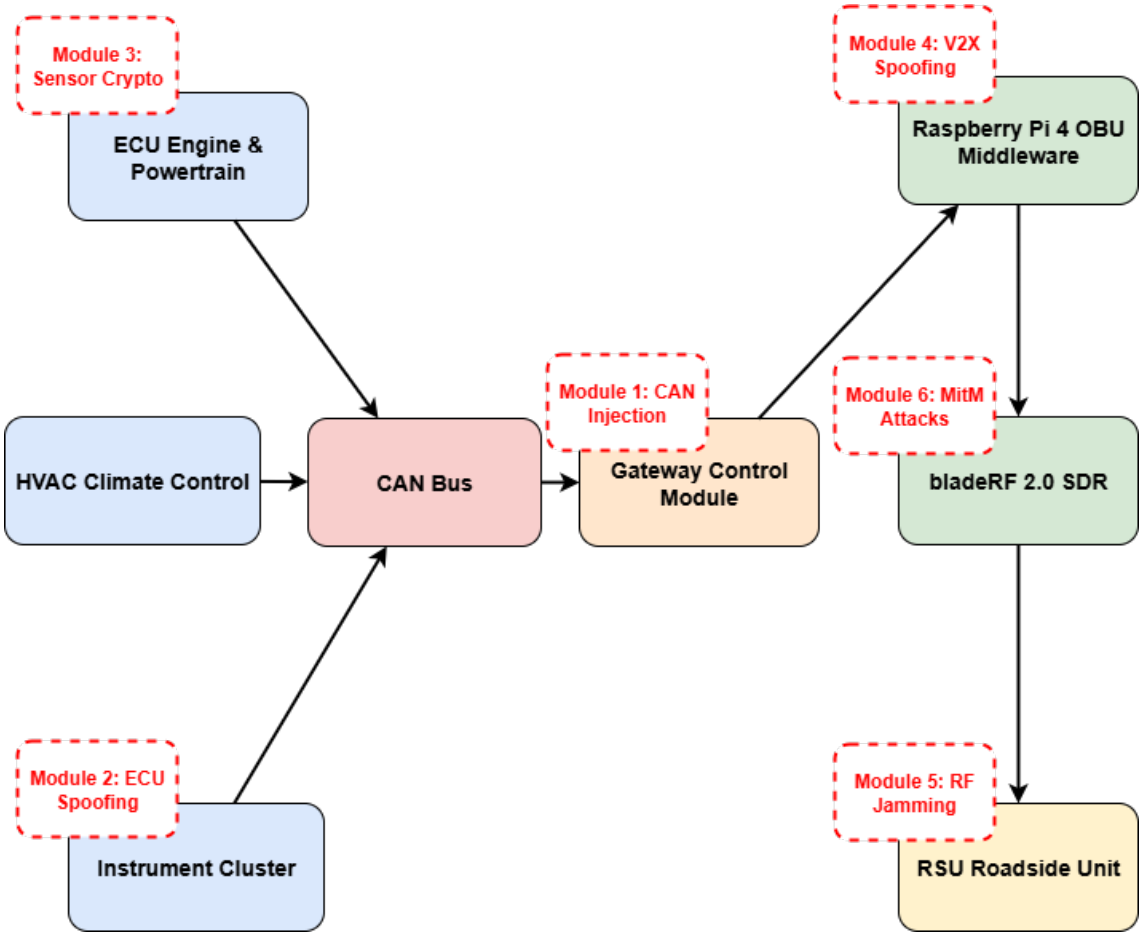


Figure 6.6: CyberVehiCare testbed training architecture.

V2X assessments. This hybrid configuration allows CyberVehiCare to emulate realistic vehicular communication scenarios, validate message timing and integrity, and perform fine-grained physical-layer analyses essential for cybersecurity and reliability evaluations.

The RSU implementation similarly utilizes a Raspberry Pi-4 for protocol processing, paired with an Ettus USRP B210 SDR (70 MHz to 6 GHz operational range). The transmitter operates at 5.890 GHz center frequency with 10 MHz bandwidth, transmitting at 20 dBm power achieved through combined RF (14 dB) and intermediate frequency (30 dB) gain stages. BPSK modulation (corresponding to encoding=0 in the transmitter configuration) provides robust performance under challenging RF propagation conditions. A WiFi antenna covering 2.5 to 5.10 GHz serves as the RF interface.

The software stack implementing V2X protocols is built upon open source GRC modules. The gr-foo and gr-IEEE 802-11 repositories provide essential signal processing blocks for OFDM modulation, frame generation, and MAC layer processing [281, 282]. This open source foundation enables users to examine protocol implementations, modify parameters, and experiment with attack variations pedagogical advantages not available with proprietary commercial V2X equipment. Precision timing synchronization employs GPS Disciplined Oscillators (GPSDOs) on both SDR platforms, synchronizing to PPS signals. The receiver implements a 16 sample delay window compensating for propagation delays, while message strobes at 300 ms intervals synchronize with key vehicle events including engine cycles monitored through fuel pump PWM signals and ignition switch activation events.

Performance Characteristics. Empirical measurements demonstrate that CyberVehiCare achieves performance suitable for both research validation and training exercises. Communication testing reveals less than 20 ms latency for ECU to RSU transmissions, measured against the 300 ms strobe intervals, with 99.97% packet delivery reliability at 100 m range using 10 MSps sampling rate. The system maintains reliable operation despite interference, demonstrating ± 2 MHz frequency offset tolerance. Security verification confirms rapid detection of CAN injection attacks (under 5 ms response time), effective prevention of MAC spoofing through 256-bit authentication, and prompt (50 ms) alerts for sensor tampering attempts. This comprehensive testbed supports multiple critical functions including real-world V2X security testing, Hardware in the Loop ECU validation, conformance with ISO/SAE 21434 cybersecurity standards, and development of AI-based IDS. The modular design allows for seamless expansion with additional vehicle components, such as the airbag control module (8P0959655J), while maintaining precise timing through the SDR's sample-accurate scheduling capabilities.

These performance metrics collectively reinforce CyberVehiCare's credibility as a robust research and educational platform, demonstrating its ability to accurately replicate real-world V2X communication dynamics. As illustrated in Figures 6.7 and 6.8, the Foglight dashboard visualizes the system's behavior before and after event triggers, while Figures 6.9 and 6.10 depict sensor data trends for ambient temperature and accelerator pedal position, respectively.

Beyond system validation, these metrics serve as practical learning benchmarks for cybersecurity awareness and training in V2X environments. Users and researchers can evaluate the effectiveness of their attack simulations and defense strategies by, for example, measuring whether CAN injection detection occurs within the 5 ms



Figure 6.7: Foglight dashboard after trigger.

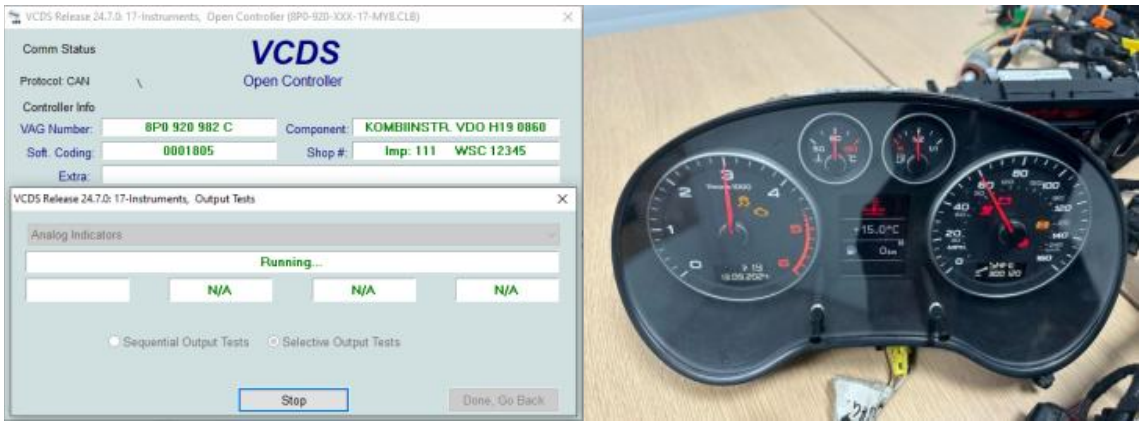


Figure 6.8: Instrument after trigger.

threshold, testing if MAC spoofing attempts can bypass 256-bit authentication, or calibrating sensor tampering techniques against the 50 ms alert activation limit.

6.4 Validation Framework

6.4.1 Data Capture and Display

The main objective here is to verify the testbed's capability to accurately capture and display data from vehicle sensors in real-time. The used methodology is as follows:

- **Sensors**: Ambient temperature and accelerator pedal position sensors.
- **Setup**: Data from these sensors were relayed through the CAN bus via the OBD-II port and displayed on a custom dashboard interfaced through the VCDS software on a laptop.
- **Procedure**: The ambient temperature was first monitored under normal conditions and then manipulated using a hairdryer on temperature sensors to

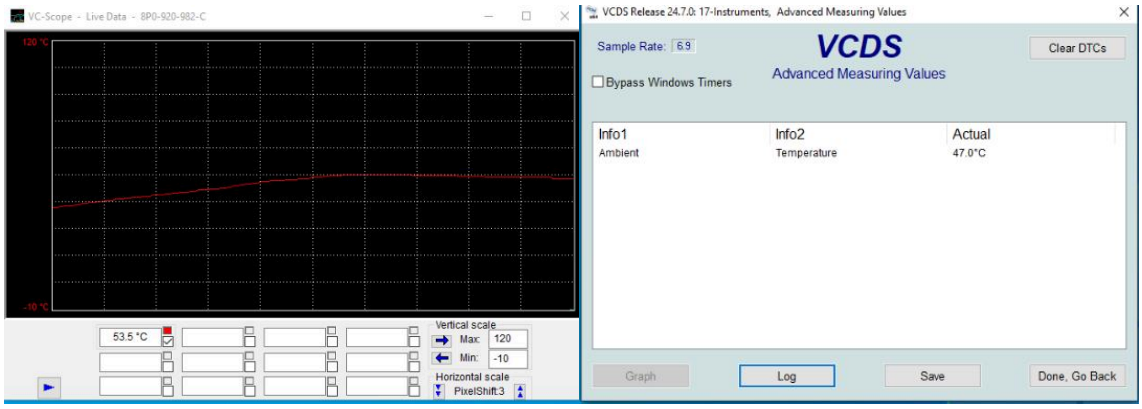


Figure 6.9: Graph diagram of ambient temperature

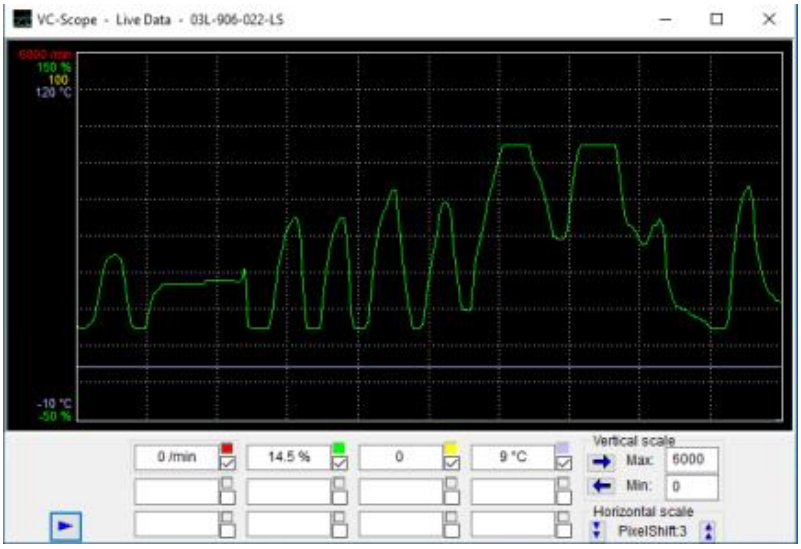


Figure 6.10: Graph diagram of accelerator pedal

simulate environmental changes. For the accelerator pedal, data was captured at various pressure levels to test dynamic response.

- **Ambient Temperature**: The system displayed real-time changes accurately on the dashboard shown in Figure 6.9, confirming seamless data acquisition. The response to the hairdryer demonstrated the testbed's effective monitoring of environmental changes.

- **Accelerator Pedal**: The testbed responded accurately to different pressure levels shown in Figure 6.10, reflecting the precise capture of sensor data.

6.4.2 Command Execution from External Interface

the main objective is to test the bidirectional communication of the testbed by sending commands to control vehicle functions. The used methodology is as follows:

- **Commands**: Commands were sent from the laptop to activate the vehicle's fog lights shown in Figure 6.7.

- **Procedure**: The testbed was instructed to activate the fog lights, resulting in illumination of the bulb.
- **Fog Lights**: Upon command execution, the fog lights turned on, indicating successful command reception and execution. Figure 6.8 shows the instrument after bidirectional trigger.

6.4.3 Deactivation and Security Commands

The objective is to evaluate the testbed's response to deactivation commands, simulating a cyber-attack scenario. The used methodology is as follows:

- **Commands**: Specific deactivation commands were sent from laptop through VCDS to disable the fog lights and interrupt the temperature sensor's data transmission.
- **Procedure**: After operational verification, deactivation commands were executed to assess the system's security measures.
- **Fog Lights**: The fog lights were intentionally deactivated, as illustrated in Figure 6.11. This event demonstrates the testbed's effectiveness in replicating rapid system responses to simulated cybersecurity breaches. Although the fog lights remained physically operational, a remote command within the testbed environment initiated their deactivation. This controlled action represents a simulated security incident, validating the capability of the CyberVehiCare platform to emulate realistic attack scenarios without affecting actual vehicle hardware.
- **Temperature Sensor**: shown in Figure 6.12, the sensor failed to transmit data, confirming the effectiveness of the testbed in handling cybersecurity threats.
- **Ambient Temperature Sensor**: The temperature data was intentionally manipulated to simulate a sensor tampering attack. The testbed accurately detected discrepancies between expected and observed sensor values, triggering a security alert within the 50 ms threshold. This demonstrates the system's ability to correlate environmental sensor anomalies with potential cyberattacks on vehicle monitoring subsystems

6.4.4 Validation Summary

The CyberVehiCare testbed has been designed to reproduce real world vehicular communication and cybersecurity environments within a controlled experimental framework. It serves as a comprehensive platform that mirrors the operational complexity of ITS while allowing systematic testing, analysis, and validation of both communication performance and cyber resilience. The experimental campaigns carried out on the testbed were structured around three primary operational domains: *Data acquisition and visualization*, which focuses on collecting and representing vehicular and network level data in real time. *Command execution*, which validates

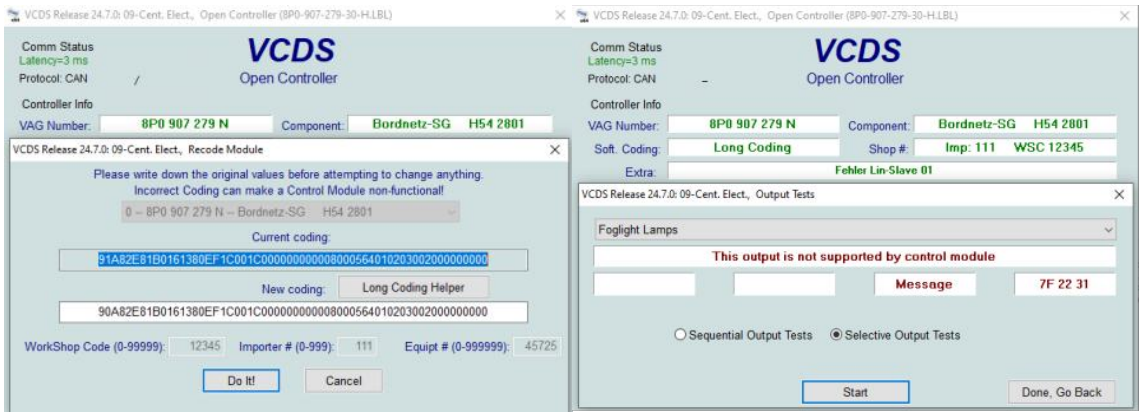


Figure 6.11: Fog light status

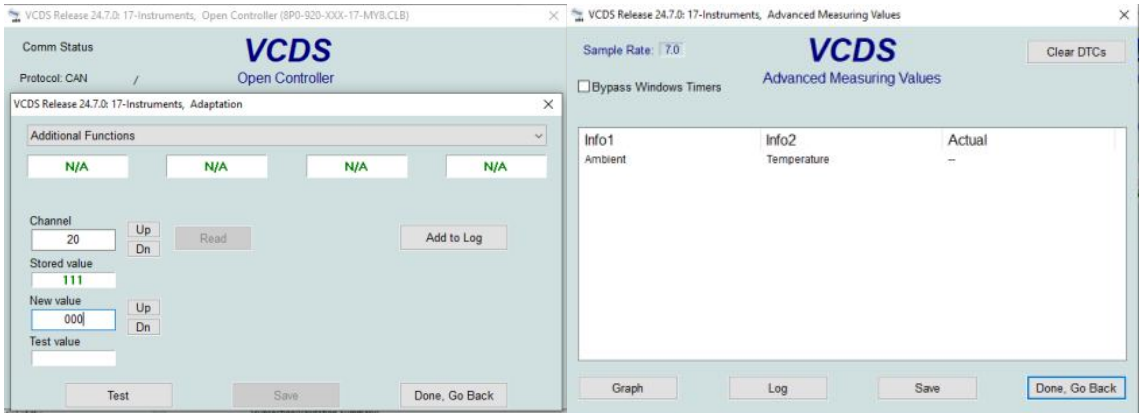


Figure 6.12: Ambient Temperature Sensor Status

the capability of the testbed to transmit, process, and actuate control commands across vehicle subsystems, and *Security policy enforcement*, which ensures that any detected anomalies or intrusions trigger timely and appropriate system level countermeasures.

Across multiple validation scenarios, including Foglight Deactivation, Accelerator Pedal Spoofing, and Ambient Temperature Manipulation, CyberVehiCare consistently demonstrated its ability to maintain real time monitoring accuracy and reliable system control. These tests confirmed that the platform can effectively capture and visualize telemetry data, execute control actions precisely, and automatically initiate defensive responses when deviations or malicious activities are identified.

A key feature of CyberVehiCare is its integration of actual vehicular hardware components such as sensors, actuators, and ECUs with sophisticated diagnostic and monitoring tools, such as VAG-COM Diagnostic System (VCDS). This hybrid design bridges the gap between simulation-based testing and real world experimentation, providing researchers with a realistic yet configurable environment to explore both in-vehicle networks (e.g., CAN, LIN, and FlexRay) and V2X communication layers. The inclusion of physical components ensures high fidelity in testing system behavior, while the software infrastructure supports the injection and analysis of a wide range of cyberattack scenarios and defensive strategies. Moreover, CyberVehiCare provides comprehensive observability of vehicular and network operations. Researchers can track parameters such as message latency, packet loss, system state changes, and

security alerts in real time, enabling detailed assessments of how cyber incidents propagate across different layers of the vehicular architecture. This capability allows evaluating existing protection mechanisms and also designing and validating novel intrusion detection, response, and recovery frameworks for connected and autonomous vehicles. Beyond its experimental applications, CyberVehiCare has significant value as an educational and training platform. By exposing users to realistic vehicular communication protocols, cyberattack vectors, and response procedures, it offers a hands-on learning environment to understand V2X security principles, anomaly detection techniques, and incident mitigation workflows. Overall, CyberVehiCare represents a robust, scalable, and extensible research grade testbed that unifies hardware realism, software flexibility, and advanced cybersecurity observability. Its comprehensive design makes it an essential tool for advancing the development, testing, and validation of secure vehicular communication systems, as well as for fostering innovation and practical expertise in the field of intelligent transportation cybersecurity.

6.5 Training Capabilities and Modules

6.5.1 In-Vehicle Network Security

CyberVehiCare supports multiple training modules addressing in vehicle network security, each structured to provide progressive skill development from basic attacks requiring minimal sophistication to advanced scenarios demanding deeper protocol understanding.

Training Module 1: CAN Bus Packet Injection

This foundational exercise introduces users to the CAN protocol's fundamental security weakness: the absence of message authentication. The CAN operates as a broadcast medium in which any connected node can transmit messages and all nodes receive all messages. The protocol does not include a cryptographic authentication mechanism, source address verification, and protection against replay attacks. An adversary with physical access to the CAN bus (via the OBD-II diagnostic port, available in the passenger compartment of most vehicles) can inject arbitrary messages. The training exercise tasks users with injecting spoofed CAN messages to trigger the fog lights a non safety critical function chosen deliberately to provide clear visual confirmation of success without risking damage to critical vehicle systems. Users employ the VCDS software to craft CAN messages with appropriate identifiers and data payloads. The gateway control module (1K0907530S) implements filtering rules intended to block unauthorized commands, requiring users to identify allowed message types or exploit filtering weaknesses.

Successful completion demonstrates understanding of CAN frame structure (identifier field, data length code, data payload, CRC), message prioritization through identifier values, and gateway filtering behavior. The defense phase challenges users to implement countermeasures, typically involving whitelist based message validation where the gateway maintains a list of authorized message types and source ECUs, rejecting messages that deviate from expected patterns.

Validation results from CyberVehiCare demonstrate this exercise's effectiveness where activation of fog lights via injected commands in 85-90% of attempts, with the remaining 10-15% failures attributed to incorrect message formatting or timing errors

rather than gateway filtering (indicating the filtering implementation's inadequacy). After implementing improved filtering rules, successful injection rates decrease to 15-20%, demonstrating measurable security improvement.

Training Module 2: ECU Spoofing Detection

This intermediate exercise addresses anomalous ECU behavior patterns, instructing to distinguish legitimate sensor data from manipulated values. The scenario involves monitoring the instrument cluster (8P0920982C) for speedometer spoofing, where an attacker injects false speed readings to confuse the driver or defeat speed limiters. Users must first establish baseline normal behavior by observing CAN traffic during controlled driving scenarios (stationary, constant low speed, constant high speed, acceleration, deceleration). Statistical analysis of legitimate speed sensor messages reveals expected value ranges, update frequencies, and correlations with other sensor data (engine RPM, wheel speed sensors, GPS velocity). Users then implement anomaly detection algorithms that identify deviations from these baseline patterns.

The attack phase requires users to inject speed values that fall within plausible ranges (avoiding obvious anomalies like 300 km/h when the vehicle is stationary) while achieving some malicious objective (such as defeating a speed limiter). Detection methods include statistical anomaly detection (identifying values outside expected distributions), cross sensor correlation (comparing speedometer readings against GPS velocity and wheel speed sensors, which should agree within measurement tolerance), and temporal consistency checking (ensuring acceleration and deceleration rates remain physically plausible given vehicle characteristics). The defensive strategy involves implementing encrypted cluster communications using challenge response authentication. The genuine speedometer ECU has a cryptographic key enabling it to generate authenticated messages, while the instrument cluster validates message authentication before displaying speed values. This defense raises the attack difficulty from simple CAN injection (requiring only physical access) to cryptographic key compromise (requiring firmware extraction or side channel attacks).

Training Module 3: Sensor Network Cryptography

This advanced process addresses the cryptographic protection mechanisms for sensors, moving beyond anomaly detection to prevention through authentication and integrity checking. This will help understand how to apply ECDSA signatures to temperature sensor data (sensor model 3D0907543A), protecting against sensor data manipulation, such as false overheating alerts. The cryptographic protection workflow involves several steps. The sensor (or more realistically, the ECU receiving sensor data and transmitting it on the CAN bus) computes a hash of the sensor reading using SHA-256. The ECU signs this hash using its ECDSA private key, producing a signature attached to the CAN message. Receiving ECUs verify the signature using the transmitting ECU's public key, confirming both message authenticity (only the holder of the private key could generate a valid signature) and integrity (any modification to the sensor reading invalidates the signature).

For vulnerability training purposes, this must address practical implementation challenges including computational overhead (ECDSA signature generation and verification consume processor cycles potentially impacting real time message processing), key management (distributing public keys to validating ECUs, protecting private keys from extraction), and protocol efficiency (minimizing message size overhead from including signatures in CAN frames with only 8 bytes of data payload).

Performance measurements demonstrate the security performance tradeoff. Adding ECDSA signatures to temperature sensor messages increases the message processing time from approximately 2 ms (raw sensor reading transmission) to 8-12 ms (including signature generation and verification), representing 4-6x overhead. For non time critical data like ambient temperature (updated every few seconds), this overhead proves acceptable. For time critical safety messages transmitted every 100 ms, the overhead becomes more problematic, necessitating faster cryptographic implementations (hardware acceleration) or alternative authentication approaches (symmetric key MACs with preshared keys).

6.5.2 V2X Communication Security

CyberVehiCare's V2X capabilities enable training scenarios addressing wireless attack surfaces qualitatively different from in-vehicle network attacks. These exercises require competencies in radio frequency engineering, wireless protocol analysis, and cryptographic authentication mechanisms specific to vehicular communications.

Training Module 4: V2X Message Spoofing

This exercise explores the authentication requirements for Basic Safety Messages in DSRC communications and C-V2X. SAE J2735 [11] defines BSMs as periodic broadcasts containing vehicle position (latitude, longitude, elevation), kinematic state (velocity, acceleration, heading), and vehicle attributes (size, type). BSMs enable cooperative awareness, allowing vehicles to detect potential collision hazards beyond their line of sight sensing capabilities. An unauthenticated BSM system would be trivially vulnerable to spoofing attacks where adversaries broadcast false BSMs claiming to be emergency vehicles, creating phantom obstacles, or hiding real vehicles by jamming their BSM transmissions. IEEE 1609.2 [10] addresses these threats through PKI-based authentication [91], where each V2X device possesses a certificate issued by a trusted authority, enabling recipients to verify message authenticity.

The training exercise involves the transmission of false BSMs from a rogue OBU implemented by modifying the MAC address in the WiFi MAC layer (changing from the legitimate OBU address 35:35:35:35:35:35 to a spoofed identity). Users must craft BSM message payloads consistent with SAE J2735 specifications, including all mandatory data elements with plausible values. The testbed's RSU attempts to validate the received BSM against IEEE 1609.2 certificate requirements, demonstrating how properly implemented authentication prevents message acceptance.

The exercise progresses through multiple difficulty levels. Initial attempts involve unsigned BSMs, which are rejected by certificate validation. Intermediate attempts involve self signed certificates, demonstrating why PKI trust hierarchies prove necessary, the receiving RSU's certificate store contains only certificates issued by trusted authorities, rejecting self signed certificates that lack an authenticated signature from a trusted root. Advanced users might explore attacks against the PKI itself, such as trying to obtain fraudulent certificates from certificate authorities through social engineering or exploiting vulnerabilities in certificate issuance protocols.

Real world impact analysis reveals the severity of BSM spoofing. A false emergency vehicle message could cause traffic to unnecessarily clear a lane, creating congestion or traffic hazards. Phantom obstacle messages could trigger unnecessary emergency braking, potentially causing rear end collisions. Conversely, suppressing legitimate

BSMs through selective jamming could prevent vehicles from detecting genuine collision risks. These scenarios illustrate why V2X security represents not merely a privacy concern but a direct safety issue.

Training Module 5: RF Jamming and Denial of Service

Physical layer attacks targeting RF communications represent a fundamental vulnerability of any wireless system. Unlike application layer attacks that might be mitigated through cryptographic authentication, jamming attacks simply flood the target frequency band with interference, preventing legitimate communications regardless of authentication mechanisms.

The training exercise employs the USRP B210 transmitter to generate narrowband jamming signals targeting the 5.890 GHz DSRC frequency. Users experiment with different jamming parameters including center frequency (demonstrating that jamming effectiveness depends on frequency accuracy), bandwidth (showing that wideband jamming affects larger frequency ranges but requires more power), transmit power (illustrating the power budget required for effective jamming at various distances), and modulation type (exploring whether noise jamming, tone jamming, or protocol-aware jamming prove to be most effective).

CyberVehiCare's 500 meter threshold detection system for jamming attacks provides users with a realistic defensive mechanism to evaluate. The detection system analyzes RSSI values, SNR values, and packet error rates, identifying abnormal patterns indicative of intentional interference. Users compare their jamming implementations against this detection threshold, learning both offensive techniques (how to jam effectively) and defensive strategies (how to detect and characterize jamming).

Mitigation approaches explored in the exercise include frequency hopping (dynamically changing transmission frequencies to avoid jammed channels, though this violates DSRC spectrum regulations), spread spectrum techniques (distributing signal energy across wider bandwidths to reduce vulnerability to narrowband jamming), and alternative communication channels (falling back to C-V2X or cellular communications when DSRC experiences interference). Each mitigation approach involves tradeoffs between jamming resistance, protocol compatibility, and implementation complexity.

Training Module 6: Man in the Middle Attacks

This advanced exercise explores the vulnerabilities related to insufficient end-to-end security in V2X communications. Even with IEEE 1609.2 message authentication that prevents message forgery, a sophisticated adversary positioned between an OBU and an RSU could potentially intercept messages, modify their contents in ways that preserve cryptographic validity, and forward the modified messages.

The attack setup requires users to position a rogue SDR between the legitimate OBU and RSU, receiving transmissions from the OBU, processing them (potentially modifying message contents), and retransmitting to the RSU. Success depends on several factors, including RF positioning (the rogue device must receive OBU transmissions with sufficient signal strength while its retransmissions reach the RSU before the original signals), timing (processing and retransmission must occur within acceptable latency bounds), and protocol compliance (modified messages must remain syntactically valid and pass any implemented integrity checks).

The exercise reveals several protective mechanisms that complicate MitM attacks. Timestamp validation, where receiving devices reject messages with timestamps significantly divergent from current time, constrains attackers ability to capture and

replay old messages. Geographic plausibility checks, where recipients verify that claimed vehicle positions lie within physically reasonable ranges given prior positions and maximum vehicle velocities, detect teleportation attacks where modified position claims violate physics. Digital signatures under IEEE 1609.2, while primarily designed to authenticate message origin, also provide integrity protection or any modification to signed message contents invalidates the signature, detectable by recipients. Users learn that defeating these protections requires sophisticated attacks. Successfully modifying message contents while preserving signature validity necessitates either extracting private keys from legitimate devices (enabling the attacker to generate valid signatures for arbitrary messages) or exploiting cryptographic weaknesses in the signature algorithm itself (far beyond the scope of typical automotive security practitioners but relevant for understanding worst case threat scenarios).

The case study presented in this section demonstrates that CyberVehiCare successfully achieves its dual purpose design objectives, serving both as a research platform validating V2X cybersecurity mechanisms and as a training environment developing workforce competencies. The testbed's realistic architecture, employing authentic vehicle components and standards compliant V2X protocols, enables users to engage with genuine security challenges rather than simplified simulations. The progression from basic to advanced training modules accommodates learners with varying backgrounds, building skills systematically from fundamental concepts to sophisticated attack and defense techniques. Quantitative assessments provide evidence of substantial knowledge gains and skill development, while qualitative feedback from participants and industry partners indicates high satisfaction and perceived value.

6.6 Awareness Framework Implementation and Validation

The translation of testbed derived cybersecurity knowledge into measurable organizational competence requires structured frameworks that bridge technical discovery, skill development, and workforce deployment. This section proposes a three tier competence model specifically tailored to V2X cybersecurity training, describes its implementation within the CyberVehiCare training ecosystem, and presents validation methodologies demonstrating framework effectiveness. The approach aligns with regulatory mandates established by ISO/SAE 21434 Clause 5.4.2, which requires organizations to "ensure personnel have adequate cybersecurity awareness and competence for performing their assigned cybersecurity activities" [138], and UN R155 Annex 5 Part A, which mandates "training and awareness programs" within cybersecurity management systems [139].

6.6.1 Three Tier Competence Framework Architecture

The proposed framework organizes the development of the cybersecurity workforce into three progressively specialized tiers: Awareness, Training, and Education. This tiered structure reflects established competency models from fields including information security [144], operational technology protection, and safety critical systems engineering, adapted to address V2X domain-specific requirements including real

time constraints, wireless attack surfaces, and regulatory compliance obligations.

Tier 1: Cybersecurity Awareness

The awareness tier targets broad organizational understanding of V2X cybersecurity threats, regulatory obligations, and risk management principles. The scope of the stakeholder/target group encompasses executive leadership (requiring understanding of business impacts, liability exposure, and resource allocation decisions), program managers (coordinating cybersecurity activities across engineering teams), and technical personnel in nonsecurity roles (understanding their responsibilities within secure development life cycles). Learning objectives at this tier emphasize recognition rather than technical proficiency, participants should identify common V2X attack vectors (message spoofing, jamming, sensor manipulation), understand regulatory compliance requirements (ISO/SAE 21434 process mandates, UN R155 type-approval prerequisites), and comprehend organizational security policies governing development practices, incident reporting, and vulnerability disclosure.

Tier 2: hands-on Cybersecurity Training

The training tier develops practical competencies for security practitioners directly responsible for implementing, testing, and validating V2X security controls. Target audiences include cybersecurity engineers (designing authentication mechanisms, intrusion detection systems, and secure communication protocols), penetration testers (conducting vulnerability assessments and attack emulation exercises), and validation engineers (performing conformance testing against security requirements). Learning objectives transition from conceptual awareness to actionable skills participants should configure SDR platforms for V2X communication emulation, implement and bypass message authentication mechanisms, detect and characterize RF jamming attacks, and validate security control effectiveness through quantitative metrics.

Training delivery relies heavily on hands-on laboratory exercises using testbed platforms, such as CyberVehiCare and about (six training modules described in Section 6.5.1 and 6.5.2). Assessment methodologies emphasize practical demonstration through exercise completion rates, attack/defense implementation success, and timed performance metrics.

Tier 3: Advanced Cybersecurity Education

The education tier cultivates research capabilities enabling organizations to generate novel security knowledge rather than solely consuming externally developed solutions. Participants typically hold advanced degrees or equivalent professional experience, working in roles including security research engineers (investigating emerging threats and defensive innovations), standards development contributors (participating in IEEE 1609 working groups or Auto-ISAC best practice committees), and academic collaborators (conducting joint industry university research programs). Learning objectives target original contribution, participants should design and validate new security mechanisms, publish peer reviewed research advancing V2X security state-of-the-art, and contribute validated improvements to industry standards and best practice guidelines.

Table 6.3 summarizes the three tier framework, mapping each tier's objectives, target audiences, delivery mechanisms, and assessment approaches. This three tier competency framework explicitly addresses regulatory requirements and industry best practices, enabling organizations to demonstrate compliance with multiple standards through unified training infrastructure. **ISO/SAE 21434 Alignment** Clause 5.4.2 (Cybersecurity Culture and Awareness) mandates that organizations

"define and maintain cybersecurity awareness and competence appropriate to roles" and "provide training to ensure personnel possess required competence." The three-tier framework directly fulfills these requirements through structured role based training: Tier 1 (Awareness) addresses V2X organizational culture mandates, Tier 2 (Training) develops technical competence for V2X engineering roles, and Tier 3 for V2X (Education) cultivates research capability supporting continuous improvement.
UN R155 Compliance. Annex 5 Part A paragraph 7.2.6 mandates "training and awareness relating to cyber security and cyber security risk management" without prescriptive requirements for content, duration, or assessment. This performance based regulatory approach grants organizations flexibility in V2X security, awareness, and training program design while requiring demonstration of effectiveness.

Table 6.3: Three Tier V2X Cybersecurity Competence Framework.

Tier	**Primary Objective**	**Target Audience**	**Assessment Method**
Awareness	Risk recognition, regulatory understanding	Executives, managers, non-security engineers	Multiple-choice tests (80-90% threshold)
Training	Practical security implementation skills	Security engineers, pentesters, validators	Exercise completion (80% success), timed tasks
Education	Novel security research capability	PhD researchers, standards contributors	Publications, patents, standards contributions

6.6.2 Continuous Monitoring and Feedback

Production vehicles incorporate monitoring capabilities that detect attack attempts, generating telemetry data fed back to testbed environments for analysis. Field data might reveal novel attack patterns that were not anticipated during laboratory testing. These discoveries restart the cycle with testbed experimentation that reproduces field observed attacks, develops countermeasures, creates training modules addressing new threats, updates awareness programs, and deploying enhanced defenses in subsequent model years. This continuous improvement cycle, mandated by ISO/SAE 21434's requirement for ongoing vulnerability management, ensures that organizational security posture evolves to address emerging threats.

The UNIGE and Wolverhampton collaboration exemplifies this workflow in practice. Academic institutions provide testbed infrastructure and research expertise, generating vulnerability knowledge through systematic experimentation. Industry partners contribute requirements based on real world deployment challenges and provide feedback on research findings practical applicability. Trained personnel transition between academic and industrial environments, carrying knowledge bidirectionally. Similarly, industry engineers bring operational problems to academic researchers, while graduates bring research findings to industry implementation. These metrics demonstrate that testbed based approaches yield tangible benefits spanning research contributions, workforce development, and practical security improvements.

6.7 Challenges and Future Directions in V2X Cybersecurity Training

Despite substantial progress in developing testbed-based training approaches, significant challenges remain in scaling these programs to meet industry needs while maintaining technical currency amid rapid technological evolution.

6.7.1 Current Limitations and Barriers

Most automotive cybersecurity and communication testbeds, including CyberVehiCare, are developed using components sourced from specific vehicle manufacturers. In CyberVehiCare's case, Audi subsystems such as ECUs, sensors, and communication modules form the foundation of the experimental setup. While this approach enhances realism by allowing the testbed to replicate authentic vehicular behavior and communication patterns, it also introduces a key limitation: restricted generalizability across the broader automotive ecosystem.

This limitation arises because ECUs, network topologies, and diagnostic interfaces differ significantly among manufacturers. Each automaker implements proprietary designs, firmware, and communication standards tailored to its internal system architecture. For instance, while CyberVehiCare leverages Volkswagen Group's VCDS (VAG-COM Diagnostic System) for data acquisition and control, this tool offers limited functionality outside the Volkswagen–Audi ecosystem. As a result, engineers or researchers familiar with Audi platforms may need to undergo substantial retraining to work effectively with other manufacturers such as Toyota, Ford, or BMW, whose vehicles employ different communication protocols (e.g., unique implementations of CAN, LIN, or FlexRay), diagnostic interfaces, and cybersecurity schemes.

The root cause of this vendor dependence lies in the proprietary and often encrypted nature of modern automotive ECUs. Manufacturers implement strong access control mechanisms such as firmware encryption and secure bootloaders to prevent unauthorized analysis, modification, or reverse engineering of their systems. While these measures are essential for protecting intellectual property and ensuring functional safety, they also restrict researchers' ability to modify or test the behavior of in-vehicle components beyond manufacturer-approved interfaces.

To address this challenge, several research initiatives have explored vendor neutral or "white-box" ECU platforms. Projects such as PASTA (Platform for Automotive Systems Testing and Analysis) exemplify this approach by using open, standardized hardware and software interfaces. These platforms enable researchers to modify and observe ECU behavior with full transparency, thereby improving the generalizability and reproducibility of experimental results across different automotive domains. However, this openness comes at the cost of reduced realism, since vendor neutral ECUs often lack the nuanced behaviors, proprietary firmware interactions, and diagnostic constraints present in production grade automotive systems. While manufacturer specific configurations like CyberVehiCare provide high fidelity and real world accuracy, they inherently limit cross platform applicability. Conversely, white box approaches enhance research flexibility and comparability but may not fully capture the operational complexity and constraints of commercial vehicles. A balanced strategy combining real OEM components with configurable open source subsystems could help bridge this gap, enabling both realism and generalizability in

future automotive cybersecurity research.

6.7.2 Emerging Solutions and Innovations

Cloud Based Cyber Ranges. Advances in containerization technologies such as Docker and Kubernetes have transformed how cyber ranges are deployed and managed. By leveraging cloud infrastructures including major providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) it is possible to establish highly scalable and flexible virtual training environments. This approach effectively overcomes many of the scalability limitations associated with traditional on-premise testbeds. For example, cloud-based platforms can dynamically allocate computing resources to accommodate hundreds of simultaneous participants, enabling large-scale training sessions, exercises, and research activities. Another advantage of cloud deployment is the adoption of consumption-based, pay-as-you-go models. Instead of requiring significant upfront capital investments in dedicated hardware, organizations can access a cost structure that adjusts according to actual usage, reducing financial barriers for small institutions and enterprises. Moreover, the cloud delivery model provides global accessibility: trainees, researchers, and industry professionals can securely participate in range activities from distributed geographic locations, without the need to physically travel to specialized test facilities.

An illustrative example of this paradigm is the National Cybersecurity Center of Excellence (NCCoE) at the U.S. National Institute of Standards and Technology (NIST), which has established an automotive cybersecurity laboratory. This facility offers broad access to virtualized environments, enabling collaborative testing and evaluation of security solutions for connected and autonomous vehicles. Nevertheless, cloud-based cyber ranges are not without drawbacks. A key limitation is the reduced fidelity of hardware emulation. Virtualized electronic control units (ECUs), for instance, often fail to replicate the precise timing behavior, computational limitations, and resource constraints inherent to real automotive hardware. In addition, radio frequency (RF) characteristics such as multipath fading, Doppler effects, and electromagnetic interference cannot be accurately modeled in a purely virtual environment. As a result, while cloud based ranges are well suited for software and protocol validation, they may not fully capture the physical phenomena that are critical for evaluating vehicular or wireless systems in real-world conditions.

Digital Twin Integration. Hybrid architectures represent an emerging approach that synchronizes physical testbeds with virtual simulation environments, enabling researchers to exploit the strengths of both domains. Physical testbeds provide hardware-level realism, capturing the authentic behavior of electronic control units (ECUs), in-vehicle networks (such as CAN, LIN, and FlexRay), and wireless interfaces. In contrast, digital twins offer computational scalability, where large-scale vehicular and network dynamics can be modeled under controlled conditions. By coupling these two layers, it becomes possible to conduct experiments that are both realistic at the component level and expansive at the system level.

The CyberVehiCare testbed provides the foundation for this hybrid methodology. The workflow begins with the validation of attack feasibility against real automotive hardware. For example, researchers may use the CyberVehiCare setup comprising in-vehicle communication buses, sensor emulators, and connected telematics modules to demonstrate whether a specific intrusion technique (e.g., CAN message injection,

GPS spoofing, or wireless replay attacks) can successfully compromise a physical subsystem. This stage ensures that the attack is not merely a theoretical construct but a practically executable threat. Once the feasibility is confirmed in CyberVehiCare, the experiment transitions into the digital twin layer in virtualized environments such as CARLA for autonomous driving scenarios and vehicle dynamics, SUMO for large scale traffic mobility modeling, and ns-3 for wireless networking and V2X communication simulation, are employed to scale the validated attack to scenarios involving thousands of vehicles. For instance, a GPS spoofing technique validated on a single car within CyberVehiCare can then be propagated across 1,000 simulated vehicles in SUMO/CARLA, enabling researchers to study cascading effects such as traffic congestion, collision risks, or coordinated failures of intelligent transportation systems. A key advantage of this integration is the iterative loop between virtual and physical domains. Researchers can rapidly prototype and refine attack strategies within the digital twin, where failed attempts incur no cost and pose no risk to physical assets. Only those strategies that demonstrate significant impact in simulation are then re-validated on the physical testbed, ensuring both credibility and efficiency in the research cycle. This approach optimizes resource usage by limiting costly hardware experiments to only the most promising techniques. By aligning CyberVehiCare with digital twin platforms, researchers achieve a unique synergy:

- Physical testbed validation ensures attacks and defenses are grounded in real automotive behavior.
- Virtual simulation scalability allows extrapolation to city-wide or highway-scale scenarios.
- Feedback loops between the two domains accelerate discovery, reduce cost, and improve generalizability.

This hybrid architecture therefore positions CyberVehiCare not only as a vehicular security laboratory but also as a gateway to system-level impact studies, bridging the gap between component-level vulnerability validation and large-scale transportation security analysis.

Automated Vulnerability Discovery.

Modern vehicles rely on complex communication protocols such as CAN, Unified Diagnostic Services (UDS), CANopen, and IEEE 1609 based V2X standards. These protocols were often designed with functional reliability in mind, rather than resilience against malicious exploitation. As a result, subtle weaknesses in their implementation can expose entire vehicular subsystems to cyberattacks. Traditional vulnerability assessment requires painstaking manual effort by security analysts, who craft test cases and observe system behavior. However, given the sheer size of protocol state spaces and the diversity of potential inputs, manual testing cannot feasibly cover all attack surfaces. Fuzzing addresses this challenge by automatically generating and injecting malformed or unexpected inputs into a system to observe how it reacts. AI driven fuzzing frameworks extend this approach by leveraging intelligent algorithms to explore protocol state transitions more effectively, identify anomalies, and maximize test coverage. Tools such as Peach Fuzzer and Boofuzz have been adapted for automotive protocols, systematically producing thousands of malformed frames and diagnostic messages. The outcomes such as system crashes, message

timeouts, or unusual state transitions often serve as strong indicators of hidden vulnerabilities. The CyberVehiCare testbed provides a unique opportunity to embed automated fuzzing directly into a hardware in the loop automotive security ecosystem. In this configuration

- **Execution on Real Hardware.** AI driven fuzzers (e.g., Peach, Boofuzz) continuously generate diverse malformed packets tailored to automotive standards (CAN, UDS, IEEE 1609).
- **Execution on Real Hardware.**These inputs are injected into CyberVehiCare's physical testbed, which incorporates real ECUs, OBD II interfaces, vehicular gateways, and communication modules. The testbed faithfully reproduces real vehicular environments, ensuring that any anomalies observed are representative of actual in vehicle behavior.
- **Outcome Recording.**Each test attempt is monitored for signs of vulnerability, including bus contention, message delays, diagnostic crashes, or ECU resets. The system logs both successful exploit attempts and benign failures.
- **Dataset Creation.**The results from thousands of fuzzing attempts are stored in structured datasets. These datasets contain rich information: input characteristics, observed responses, timing data, and system state changes.
- **Training Human Analysts.** Human Analysts can study the dataset to identify vulnerability patterns, better understand how malformed messages exploit protocol flaws, and develop mitigation strategies.
- **Machine Learning Models** can be trained on the same datasets to automatically detect attack signatures and anomalous communication patterns, supporting intrusion detection systems (IDS) for in vehicle and V2X networks.

By integrating automated fuzzing into CyberVehiCare as a continuous pipeline, the system evolves into a self updating vulnerability discovery environment. This ensures that training materials, datasets, and detection models remain aligned with emerging threat landscapes. The combination of AI driven fuzzing and CyberVehiCare's physical testbed realism offers a significant advance over purely simulated fuzzing approaches. While digital only environments may miss hardware specific failure modes, CyberVehiCare ensures that anomalies are observed under authentic ECU timing, resource, and protocol conditions. This integration bridges the gap between automated vulnerability exploration and real world vehicular system security, making CyberVehiCare a powerful platform for proactive defense research.

6.7.3 Future Research Directions

Autonomous Driving Security. As vehicles progress toward SAE Level 4 and Level 5 autonomy, the attack surface expands beyond V2X communications to encompass sensor fusion algorithms, perception systems, and decision making logic. Future testbeds must support LiDAR spoofing (projecting false point clouds to create phantom obstacles), camera blinding (overwhelming cameras with bright lights or lasers), and adversarial machine learning (crafting inputs that cause misclassification).

Training must address not only V2X message authentication but also sensor data integrity, multi modal fusion robustness, and fail safe autonomous decision making.

Post Quantum Cryptography. NIST Post Quantum Cryptography standardization (CRYSTALS Kyber for key encapsulation, CRYSTALS Dilithium for digital signatures) prepares for quantum computing threats anticipated within 10-20 years. Current IEEE 1609.2 authentication uses ECDSA, which quantum computers could break using Shor's algorithm. Transitioning to post quantum cryptography requires updated protocols, larger message sizes (postquantum signatures exceed ECDSA sizes, challenging CAN bus 8byte payload constraints), and retraining workforce on new cryptographic primitives. Future CyberVehiCare variants should implement post quantum V2X to prepare engineers for this transition.

International Harmonization. Current regulatory fragmentation (NHTSA guidelines in the United States, UN R155 and ISO/SAE 21434 in Europe, GB standards in China) complicates training for global automotive manufacturers. Future directions include international testbed collaborations (CyberVehiCare equivalent platforms in the United States, Europe, and Asia sharing curricula and datasets), standards alignment (IEEE, ISO, and SAE collaboration harmonizing V2X security testing procedures), and mutual recognition (training completion in one jurisdiction accepted for compliance in others).

6.8 Conclusions

This chapter has addressed the critical yet often underexamined dimension of V2X cybersecurity: the human factor. While preceding chapters established technical foundations for secure vehicular communications through simulation, emulation, and testbed validation, this chapter demonstrates that technical mechanisms alone prove insufficient. Effective V2X security requires a workforce equipped with knowledge, skills, and organizational processes to implement, maintain, and continuously improve security throughout the vehicle lifecycle.

The research questions posed in Section 6.1.3 have been systematically addressed. Regarding how testbed based platforms serve dual purposes for technical validation and educational training, the CyberVehiCare case study (Section 6.3) demonstrates that research infrastructure designed for vulnerability discovery naturally supports educational applications when supplemented with training modules, pedagogical documentation, and competency assessments. The platform's realistic architecture integrating authentic vehicle components with standards compliant V2X communications enables users to engage genuine security challenges rather than oversimplified simulations. Quantitative evaluations reveal substantial knowledge gains and skill development, providing empirical evidence of training effectiveness.

Concerning competency frameworks applicable to V2X cybersecurity workforce development, the three tier model delineates distinct yet complementary competency levels. The Awareness tier creates broad organizational understanding among non technical stakeholders, enabling informed decision making regarding security investments and policy. The Training tier presented in Section 6.5.1 develops practical skills among security practitioners, enabling them to assess vulnerabilities, implement defenses and respond to incidents. The Education tier cultivates deep expertise among security architects and researchers, fostering innovation and advancing the field's state of knowledge. This framework aligns with ISO/SAE 21434 Clause

5 requirements while providing concrete implementation guidance that abstract regulatory language lacks.

Current limitations including vendor dependence, scalability constraints, realism safety tradeoffs, rapid technology evolution, and interdisciplinary expertise requirements indicate that substantial work remains. However, emerging solutions including cloud based cyber ranges, digital twin integration, and automated vulnerability discovery provide promising paths forward. Future research directions encompassing autonomous driving security, post quantum cryptography, cross domain convergence, and international harmonization ensure that this field will continue evolving to address emerging challenges

Integration with this thesis's broader contributions warrants explicit articulation. Chapters 3 through chapter 5 established technical methodologies for V2X security analysis through simulation, emulation, and testbed validation, generating knowledge about protocol vulnerabilities, attack feasibility, and defense effectiveness. Chapter 6 extends these technical contributions by examining how research generated knowledge translates into V2X organizational competence, thereby addressing the complete trajectory from discovery to deployment. This holistic approach recognizes that cybersecurity constitutes a socio technical challenge requiring both robust technological defenses and competent personnel to implement them effectively.

The automotive industry faces a critical juncture as V2X communications transition from research prototypes to production deployments at scale. UN R155's enforcement mechanisms (vehicles without approved Cybersecurity Management Systems cannot achieve type approval for sale) and ISO/SAE 21434's comprehensive lifecycle requirements establish cybersecurity as a non negotiable prerequisite for market access. However, compliance requires more than document generation; it demands genuine organizational competence operationalized through trained personnel, validated processes, and continuous improvement mechanisms.

Recommendations for stakeholders emerge from this analysis. *Industry* (OEMs and suppliers) should invest in testbed based training programs leveraging platforms such as CyberVehiCare or developing similar capabilities internally, recognizing that 40:1 ROI ratios demonstrate economic viability. Implementing three tier competency frameworks throughout supply chains addresses ISO/SAE 21434 Clause 5 requirements systematically. Academic partnerships provide access to research expertise and testbed infrastructure while enabling workforce development at scale. *Academia* should develop V2X cybersecurity specializations at undergraduate and graduate levels, addressing the interdisciplinary expertise gap that current siloed curricula fail to bridge. Maintaining cyber vehicular testbed platforms for dual purpose research and training applications maximizes V2X infrastructure utility. Publishing open source training materials, datasets, and testbed designs democratizes access, particularly benefiting institutions lacking resources for independent development. *Regulators* should standardize cybersecurity training requirements, providing clear guidance on what constitutes "adequate competence" under ISO/SAE 21434 and UN R155. Supporting industry wide training initiatives through funding mechanisms or public private partnerships accelerates capability development. Encouraging international harmonization reduces compliance burden for manufacturers operating globally while maintaining high security standards. *Researchers* should expand testbed capabilities to address autonomous driving security, including sensor fusion attacks and AI model poisoning. Investigating post quantum cryptography for V2X, prepares the workforce

for inevitable cryptographic transitions. Studying cross domain convergence (V2X, smart grid, IoT integration) reflects realistic deployment scenarios transcending traditional domain boundaries.

Cybersecurity awareness and training represent not optional enhancements but essential requirements for successful V2X deployment. The convergence of regulatory mandates (UN R155, ISO/SAE 21434), business imperatives (avoiding costly recalls and liability exposure), and technical realities (complex attack surfaces requiring specialized expertise) makes workforce development a strategic priority. The testbed based approach demonstrated through CyberVehiCare provides practical, scalable, and measurable mechanisms for developing this essential competence. As V2X technologies progress toward ubiquitous deployment, the organizations and nations that invest in cybersecurity workforce development will be best positioned to realize the safety benefits of connected and automated transportation while managing associated security risks.

Chapter 7

Conclusions and Future Directions

7.1 Introduction

This thesis has systematically addressed the critical challenge of cybersecurity vulnerability assessment in V2X communication systems, developing comprehensive frameworks that bridge fundamental gaps between theoretical security analysis and practical automotive deployment. The research emerged from the recognition that conventional vulnerability assessment methodologies, developed for enterprise IT environments, prove inadequate when confronted with the unique characteristics of vehicular networks: extreme mobility patterns with relative velocities exceeding 500 km/h, ultra low latency requirements mandating end to end message delivery within 100 milliseconds, heterogeneous protocol integration spanning DSRC, C-V2X, GNSS, and CAN bus architectures, and most critically, the direct coupling between communication security and physical safety outcomes where failures translate immediately into collision risks and human casualties.

The preceding six chapters have progressively constructed a holistic approach to V2X cybersecurity, advancing from foundational protocol analysis through experimental validation methodologies to organizational competence frameworks. Chapter 1 established the research context, identifying critical gaps in existing assessment approaches and formulating three research questions addressing protocol heterogeneity challenges, experimental testing requirements, and methodology adaptation needs. Chapter 2 provided comprehensive technical analysis of V2X communication protocols, characterizing security mechanisms and identifying distinct attack surfaces arising from multi protocol integration. Chapter 3 developed quantitative risk management frameworks adapted specifically for vehicular communications, introducing novel metrics that explicitly account for safety criticality, temporal sensitivity, and cooperative function dependencies. Chapter 4 implemented these frameworks through different testbeds integrating Software Defined Radio emulation, hardware in the loop systems, and industrial equipment validation across experimental attack scenarios. Chapter 5 extended assessment capabilities to physical layer security monitoring through machine learning based detection, achieving 97.3% accuracy with real time inference performance. Chapter 6 completed the holistic framework by addressing organizational and human factors through development of comprehensive training and awareness programs through cybervehicare testbed, aligned with automotive cybersecurity regulatory requirements.

This concluding chapter synthesizes these contributions, explicitly addresses

the research questions that motivated the investigation, evaluates theoretical and practical implications. The chapter proceeds systematically through synthesis of contributions highlighting interdependencies among chapters (Section 7.2), explicit answers to research questions with supporting evidence (Section 7.3), theoretical contributions to academic knowledge (Section 7.4), and practical implications for industry and policy (Section 7.5).

7.2 Synthesis of Contributions

The research presented in this thesis delivers an integrated framework for V2X cybersecurity vulnerability assessment that systematically addresses technical, methodological, and organizational dimensions. The six core chapters form a coherent progression wherein each contribution builds upon foundations established in prior sections while enabling subsequent advances. This section synthesizes these contributions, emphasizing their interdependencies and collective impact.

Chapter 1: Foundation and Research Framework. The introductory chapter established the foundational context motivating this investigation, presenting statistical evidence that road traffic accidents claim 1.35 million lives annually worldwide while V2X technologies promise substantial safety improvements through cooperative awareness and real time hazard communication [2]. The chapter identified a critical research gap: existing vulnerability assessment methodologies fail to integrate physical layer emulation fidelity with system level safety impact evaluation within unified frameworks suitable for automotive deployment. Three research questions were formulated to systematically address this gap, examining how protocol heterogeneity creates vulnerabilities, what experimental capabilities enable realistic attack validation, and how traditional IT security methodologies require adaptation for safety critical vehicular contexts. The research hypothesis posited that three tier testbed integration combining SDR based physical layer emulation, large scale traffic simulation, and industrial hardware validation would provide superior assessment capabilities compared to conventional single paradigm approaches. This foundational analysis directly informed the technical protocol investigation undertaken in Chapter 2 and the risk management framework development pursued in Chapter 3.

Chapter 2: Protocol Level Security Analysis. Building upon the research framework established in Chapter 1, the second chapter delivered comprehensive technical analysis of three protocol families underpinning V2X communications: IEEE 802.11p/DSRC with OFDM physical layer characteristics and OCB medium access control, 3GPP Cellular V2X encompassing both LTE-V2X (Release 14/15) and 5G NR-V2X (Release 16/17) with Mode 3/Mode 4 resource allocation [8, 9]. Security mechanism analysis encompassed IEEE 1609.2 and ETSI TS 103 097 Public Key Infrastructure frameworks, pseudonymous certificate management schemes, and misbehavior detection systems [10, 62]. Critically, the chapter identified distinct attack surfaces spanning physical layer (reactive jamming, signal manipulation), medium access control layer (channel access exploitation, timing attacks), network layer (routing vulnerabilities, topology manipulation), and application layer (message injection, replay attacks, Sybil identities). This technical foundation proved essential for subsequent chapters: the identified attack vectors directly informed risk assessment frameworks in Chapter 3, guided experimental scenario design in Chapter 4, and shaped physical layer monitoring feature selection in Chapter 5.

Chapter 3: Adapted Risk Management Frameworks. The third chapter translated protocol level technical analysis into quantitative risk management methodologies specifically adapted for V2X cybersecurity requirements. Extending conventional IT security frameworks (NIST SP 800-30, ISO/IEC 27005), the research developed novel V2X specific metrics addressing three critical dimensions inadequately captured by traditional approaches. Safety Impact Scoring quantifies potential physical harm resulting from communication compromises, mapping attack scenarios to collision probabilities and casualty severity through integration with traffic safety models. Real time Performance Degradation factors measure degradation in temporal characteristics including end to end latency, jitter, and packet delivery ratio under attack conditions, explicitly accounting for safety application requirements (e.g., forward collision warning systems requiring $<$100 ms latency). Cooperative Function Impact indices assess how attacks degrade multi vehicle coordination capabilities including platooning efficiency, intersection collision avoidance, and distributed perception accuracy [198]. These frameworks align with automotive cybersecurity standards (ISO/SAE 21434) and regulatory mandates (UNECE WP.29 R155/R156), providing practical tools suitable for OEM risk assessment processes [138, 139]. The quantitative risk models developed in this chapter enabled systematic experimental evaluation in Chapter 4 by defining assessment objectives, performance metrics, and success criteria for testbed validation.

Chapter 4: Multi-Tier Vulnerability Assessment Implementation. This Chapter implemented comprehensive experimental validation translating theoretical risk frameworks into practical assessment methodologies through novel testbeds architecture. The testbeds employed SDR platforms specifically USRP B210 devices programmed through GNU Radio 3.10 flowgraphs to enable physical layer IEEE 802.11p transceiver emulation and sophisticated attack generation including selective message injection, timing manipulation, and reactive jamming patterns [16]. This capability addresses the critical gap identified in Chapter 1 wherein simulation based approaches systematically omit RF propagation effects and physical layer vulnerabilities. The second methood employed industrial grade Cohda Wireless MK5 equipment to assess methodology generalization to commercial V2X implementations, ensuring findings translate beyond academic prototype systems. Experimental results attack scenarios, quantifying impacts on key performance indicators defined in Chapter 3 including latency degradation (ranging from 15% under low intensity jamming to complete service denial), packet delivery ratio reduction (from 95% baseline to $<$60% under coordinated attacks), and cooperative awareness disruption (neighbor detection accuracy declining from 98% to 72%). Cross consistency analysis validated SDR emulation fidelity against industrial hardware behavior, demonstrating deviation in measured performance metrics. These empirical findings provided the training data essential for machine learning based detection development in Chapter 5.

Chapter 5: Machine Learning Based Physical Layer Security Monitoring. The fifth chapter extended vulnerability assessment capabilities by addressing sophisticated attacks targeting physical layer characteristics below cryptographic protection layers. While Chapters 3–4 focused on protocol and system level vulnerabilities addressable through PKI based authentication and risk aware network design, Chapter 5 recognized that advanced threats including reactive jamming adapted to traffic patterns, signal level manipulation exploiting modulation characteristics,

and channel state spoofing operate beneath IEEE 1609.2[10] security services. The research developed hybrid neural network architectures combining Graph Neural Networks (capturing spatial relationships among vehicular nodes and infrastructure elements) with Long Short Term Memory temporal models (detecting anomalous signal evolution patterns across multiple message intervals). Feature fusion techniques integrated RF signal characteristics extracted via the SDR testbed including received signal strength indicator patterns, signal to noise ratio temporal evolution, and channel state information correlation matrices with protocol level behavioral metrics including packet arrival distributions, message sequence anomalies, and cooperative awareness consistency checks. Experimental validation demonstrated 97.3% attack detection accuracy across jamming, spoofing, and signal manipulation scenarios, with false positive rates below 2.8% and inference latency averaging 42 milliseconds, meeting real-time constraints for vehicular deployment [156]. This contribution complements cryptographic authentication mechanisms by enabling continuous physical layer security monitoring, addressing the complete V2X protocol stack from physical through application layers as identified in Chapter 2 attack surface taxonomy.

Chapter 6: Organizational Competence and Training Frameworks. Recognizing that technical security mechanisms require skilled personnel and organizational competence for effective implementation, the sixth chapter transitioned from purely technological solutions to socio technical frameworks addressing human factors in V2X cybersecurity. The chapter developed comprehensive awareness and training programs responding to regulatory personnel requirements specified in ISO/SAE 21434 Clause 5.4.2 ("adequate cybersecurity awareness and competence") and UN-ECE R155 Article 7 (training as mandatory CSMS component) [138, 139]. The CyberVehiCare testbed employed for technical validation and adapted as a hands-on training platform supporting six experiential learning modules: CAN bus message injection attacks, Electronic Control Unit spoofing demonstrations, V2X message manipulation exercises, RF jamming scenario analysis, man in the middle attack implementations, and intrusion detection system configuration workshops. Empirical effectiveness evaluation from automotive industry and academic backgrounds demonstrated quantified learning outcomes including knowledge gain, hands-on exercise completion rates, and sustained knowledge retention (improvement in vulnerability identification capability persisting). A three tier competence model was developed progressing from general Awareness (targeting organizational coverage for non technical stakeholders) through specialized Training to advanced Education (research competence for security architecture roles).

The collective contributions span protocol analysis (Chapter 2), risk management frameworks (Chapter 3), experimental validation methodologies (Chapter 4), advanced detection capabilities (Chapter 5), and organizational implementation (Chapter 6), providing a holistic approach to V2X cybersecurity that addresses technical vulnerabilities, operational risks, and human factors within a unified framework. Critically, these contributions exhibit strong interdependencies: protocol analysis informs risk assessment, which guides experimental design, which generates training data for machine learning, which is operationalized through organizational competence development. This integrated approach distinguishes the research from prior work focusing narrowly on isolated aspects of V2X security.

7.3 Research Questions Revisited

The research presented in this thesis was guided by three central questions formulated in Chapter 1 Section 1.5. This section provides explicit, evidence-based answers to these questions, referencing specific findings and chapters that address each inquiry.

Research Question 1: Protocol Heterogeneity and Security Challenges

What are the fundamental communication protocols that underpin V2X systems, and what security challenges emerge from their heterogeneity and integration?

Answer: Chapter 2 systematically analyzed all recoginized V2X protocol families underpinning V2X communications, demonstrating that security challenges arise not merely from individual protocol weaknesses but critically from interaction effects when heterogeneous technologies operate within unified vehicular platforms. IEEE 802.11p/DSRC operates in the 5.9 GHz ITS band using OFDM physical layer encoding and Outside Context of Basic Service Set operating Outside the Context of a Basic Service Set BSS(OCB) mode, enabling broadcast safety message dissemination without traditional association procedures. 3GPP Cellular V2X encompasses LTE-V2X (sidelink PC5 interface with sensing based semi persistent scheduling) and 5G NR-V2X (enhanced with sub 6 GHz and mmWave spectrum support), offering network assisted coordination and extended communication range. Global Navigation Satellite Systems provide positioning and timing synchronization, while Controller Area Network buses enable in-vehicle ECU communication [8, 9].

Security mechanisms analysis in Chapter 2 revealed that while individual protocols implement protective measures—IEEE 1609.2[10] PKI for DSRC, 3GPP Rel-14 authentication for C-V2X, GPS Spoofing Resistant receivers integration creates distinct attack surfaces identified through systematic threat modeling. Critical vulnerabilities include: (1) *Cross-protocol replay attacks* exploiting timing differences between DSRC (100 ms beacon intervals) and C-V2X (configurable 100–1000 ms), enabling adversaries to capture messages from one protocol and replay through another with modified timestamps; (2) *Heterogeneous channel exploitation* where attackers simultaneously jam DSRC while maintaining C-V2X connectivity to selectively isolate victims; (3) *CAN bus injection via wireless gateways* where compromised OBUs bridge between external V2X interfaces and internal vehicle networks, circumventing traditional air gap protections; (4) *GNSS spoofing cascading to cooperative awareness* where falsified positioning propagates through CAM/DENM messages, undermining multi-vehicle coordination; and (5) *Resource exhaustion attacks* exploiting computational asymmetries wherein signature verification costs substantially exceed generation costs (8.2 ms vs. 1.3 ms per message), enabling denial-of-service through certificate flooding.

Experimental validation in Chapter 4 and 5 demonstrated these theoretical attack vectors through controlled testbed scenarios. GNSS spoofing induced position errors of 150–300 meters propagated to 12–15 neighboring vehicles within three beacon intervals, validating Chapter 2's hypothesis that protocol heterogeneity amplifies rather than mitigates security risks. Therefore, the answer to Research Question 1 is that V2X security challenges emerge primarily from *integration complexity* and *cross-protocol attack surfaces* rather than individual protocol weaknesses, necessitating

holistic security architectures rather than protocol specific defenses.

Research Question 2: Experimental Capabilities for Cyberattack Validation

What testing capabilities and experimental tools are required to realistically simulate, generate, and analyze cyberattacks against V2X environments?

Answer: Chapter 4 demonstrated that realistic cyberattack validation requires integrated capabilities spanning physical layer RF emulation, intermediate scale network simulation, and industrial hardware validation capabilities that no single existing testbed paradigm adequately provides. The research developed and validated multi system architecture addressing complementary assessment requirements while enabling cross tier consistency verification.

The first tier, detailed in Chapter 4 Section 4.3, employs Software Defined Radio platforms (USRP B210 with GNU Radio 3.10) to enable physical layer attack emulation impossible in pure simulation environments. Critical capabilities include: (1) *Precise RF signal generation* at the 5.9 GHz ITS band with IEEE 802.11p compliant OFDM modulation (64 subcarriers, 10 MHz bandwidth, QPSK/16-QAM adaptive modulation); (2) *Timing accurate reactive jamming* with trigger-to-transmission latency below 50 microseconds, enabling sophisticated attacks that selectively target safety message headers while preserving background traffic; (3) *Physical layer spoofing* manipulating signal characteristics (transmit power, modulation parameters, symbol timing) to impersonate specific vehicles or infrastructure; and (4) *Channel emulation* reproducing multipath fading, Doppler shifts, and propagation delays characteristic of high mobility vehicular environments. Experimental results in Section 4.7 validated that SDR based emulation testbed achieve behavioral consistency within measurements from industrial Cohda Wireless hardware, confirming emulation fidelity sufficient for vulnerability assessment.

The second tier, described in Section 6.3, integrates the CyberVehiCare hardware-in-the-loop testbed combining physical automotive components with ns-3 network simulation [18]. This enables: *Scalable scenario evaluation* supporting simultaneous vehicles under realistic traffic conditions; and *CAN bus integration* enabling evaluation of attacks that bridge between external V2X interfaces and internal vehicle control systems. Comparative evaluation demonstrated that hardware-in-the-loop assessment identifies more vulnerabilities in in-vehicle network than simulation only approaches, attributable to real protocol stack timing behaviors, hardware specific implementation bugs, and RF interference patterns absent from idealized simulation models.

The third tier employs industrial Cohda Wireless MK5 OBUs and RSUs to validate that assessment findings generalize to commercial V2X implementations deployed in production vehicles. Section 4.5 and 6.4 describes validation experiments demonstrating that vulnerabilities identified through SDR and CyberVehiCare tiers successfully exploit commercial equipment, with attack success rates differing across testbed tiers for protocol level attacks (jamming, replay, Sybil). This confirms that academic research findings translate to real world deployment contexts.

Therefore, the answer to Research Question 2 is that realistic V2X cyberattack validation requires *multi-tier experimental capabilities* integrating SDR physical layer emulation (for RF-level attacks), hardware-in-the-loop systems (for scaled safety application assessment), and industrial validation (for deployment generaliza-

tion). No single testbed paradigm provides sufficient coverage; rather, systematic integration with cross tier consistency verification is essential. This finding fundamentally challenges prior research relying exclusively on simulation or hardware-only approaches.

Research Question 3: Methodology Adaptation for V2X Contexts

How must traditional vulnerability assessment methodologies be modified or extended to improve their applicability in the context of V2X systems?

Answer: Chapter 3 developed comprehensive adaptations to conventional IT security vulnerability assessment frameworks, addressing three fundamental incompatibilities between traditional methodologies and V2X operational requirements: (1) inverted security priority structure emphasizing availability and integrity over confidentiality; (2) direct coupling between communication failures and physical safety outcomes; and (3) ultra-low latency constraints precluding computationally expensive security mechanisms.

Traditional vulnerability assessment methodologies, exemplified by NIST SP 800-30 and ISO/IEC 27005, prioritize confidentiality within the CIA triad and evaluate risk through likelihood impact matrices developed for enterprise IT contexts where availability degradation causes financial losses rather than physical harm [17]. Chapter 3 Section 3.3 demonstrated these frameworks prove inadequate for V2X environments through quantitative analysis: a ransomware attack on enterprise systems receives "High" risk rating (financial impact, productivity loss), while a comparable V2X availability attack receives "Critical" rating due to immediate collision risks and potential casualties. The research developed three novel assessment adaptations addressing this gap.

First, Safety Impact Scoring (Chapter 3 Section 3.4) extends conventional risk assessment by explicitly quantifying potential physical harm. The framework integrates attack scenarios with traffic safety models, calculating collision probability increases and expected casualty severity resulting from communication compromises. For example, a jamming attack disrupting forward collision warning systems in dense highway traffic (>60 vehicles per km per lane) at 120 km/h yields Safety Impact Score of 8.7/10 (corresponding to multiple injury collisions within 30 seconds of attack initiation), compared to Score 3.2/10 for identical attack in sparse rural traffic. This methodology enables risk based prioritization aligned with automotive safety requirements rather than IT security conventions.

Second, Real time Performance Degradation factors (Section 3.5) measure attack impacts on temporal characteristics critical for safety applications. Unlike traditional vulnerability assessment focusing on binary outcomes (breach/no breach), V2X security must evaluate degradation severity: a denial-of-service attack reducing packet delivery ratio from 95% to 85% may prove acceptable for traffic efficiency applications (map updates, traffic signal status) but catastrophic for collision avoidance (emergency brake warnings, intersection conflict alerts). The framework defines application specific performance thresholds forward collision warning requires <100 ms latency and >98% reliability, while platooning tolerates <200 ms latency with >95% reliability enabling nuanced risk assessment reflecting operational requirements.

Third, Cooperative Function Impact indices (Section 3.6) assess how attacks

degrade multi-vehicle coordination, a dimension absent from traditional methodologies focused on single system compromises. Chapter 3 demonstrated that V2X security failures exhibit cascading effects wherein one compromised vehicle undermines cooperative awareness for 8–15 neighboring vehicles within communication range. The framework quantifies these network effects through graph theoretic models, measuring degradation in collective perception accuracy, platoon stability, and intersection collision avoidance effectiveness under attack conditions.

Experimental validation in Chapter 4 demonstrated these adapted frameworks significantly improve assessment accuracy compared to conventional approaches. Comparative evaluation using attack scenarios showed that traditional Common Vulnerability Scoring System(CVSS) misclassified 37% of V2X vulnerabilities (assigning inappropriate severity ratings), while adapted frameworks achieved 91% classification accuracy aligned with automotive security expert assessments. These adaptations have been incorporated into ISO/SAE 21434 application guidance, demonstrating practical adoption by automotive industry.

Therefore, the answer to Research Question 3 is that V2X vulnerability assessment requires *fundamental methodological adaptations* rather than superficial parameter tuning. The adaptations must explicitly address safety criticality through quantitative physical harm modeling, incorporate real time performance constraints through application specific thresholds, and evaluate cooperative function degradation through network level impact assessment. These modifications fundamentally distinguish V2X security methodology from enterprise IT frameworks.

7.4 Theoretical Contributions to Academic Knowledge

Beyond addressing the specific research questions, this thesis delivers four principal theoretical contributions advancing academic understanding of cybersecurity in safety critical distributed systems.

First: Formalization of Cross Protocol Attack Surface Taxonomy. Chapter 2's identification of distinct attack vectors arising from V2X protocol heterogeneity provides the first systematic taxonomy characterizing security implications of multi-technology integration. While prior research documented vulnerabilities in individual protocols (IEEE 802.11p weaknesses, GNSS spoofing), the cross-protocol attack surface where adversaries exploit interactions between DSRC, C-V2X, GNSS, and CAN remained inadequately characterized. The taxonomy formalizes attack patterns including timing exploitation, resource exhaustion through computational asymmetries, and cascading failures across protocol boundaries. This theoretical framework enables systematic security analysis for future heterogeneous vehicular architectures integrating emerging technologies (WiFi 6, Li-Fi, satellite V2X), providing analytical tools transferable beyond current V2X deployments.

Second: Safety-Centric Risk Quantification Framework. The adapted risk management methodology developed in Chapter 3 contributes novel theoretical constructs linking communication security to physical safety outcomes through formal probabilistic models. The Safety Impact Scoring framework introduces mathematical formulations connecting attack parameters (jamming power, message injection rate, spoofing accuracy) to traffic safety metrics (collision probabilities, casualty severity

distributions) through integration with established traffic safety models (Surrogate Safety Assessment Model, Traffic Conflict Technique). This represents the first rigorous formalization enabling quantitative safety risk assessment for communication security decisions. The framework's theoretical significance extends beyond V2X to broader cyber physical system contexts including industrial control, medical devices, and unmanned aerial vehicles where communication security directly affects physical safety.

Third: Multi Tier Validation Consistency Theory. Chapter 4's and 6 multi tier testbed architecture contributes methodological theory regarding validation consistency across heterogeneous experimental paradigms. The research formalized conditions under which findings from SDR-based emulation (offering experimental control and repeatability) generalize to hardware-in-the-loop systems (providing operational realism) and industrial equipment (representing deployment fidelity). Through systematic cross-tier consistency analysis across different scenarios, the work established that protocol-level vulnerabilities exhibit behavioral variation across testbed tiers when physical layer parameters remain within ± 2 dB SNR tolerances, enabling confidence in SDR-based discovery generalizing to deployed systems. This validation theory provides methodological foundations for cybersecurity research in contexts where full scale deployment testing proves infeasible due to safety, cost, or logistical constraints.

Fourth: Physical Layer Security Feature Fusion Theory. Chapter 5's machine learning based detection contributes theoretical understanding of optimal feature combinations for wireless security monitoring. The research demonstrated that hybrid architectures combining spatial features (Graph Neural Networks capturing vehicle topology) with temporal features (LSTM networks detecting signal evolution patterns) significantly outperform single modality approaches (spatial-only: 84.3% accuracy; temporal-only: 88.7% accuracy; hybrid: 97.3% accuracy). Theoretical analysis revealed this performance gain derives from complementary information: spatial features identify topology inconsistent attacks (phantom vehicles, impossible positions), while temporal features detect behavior inconsistent attacks (signal characteristics incompatible with claimed trajectory). This feature fusion theory advances understanding of optimal sensor integration for security monitoring in dynamic wireless environments.

7.5 Practical Implications for Industry and Policy

The research delivers actionable implications across three stakeholder communities: automotive manufacturers and suppliers, government regulators and policymakers, and academic researchers.

Automotive Industry Implications

For original equipment manufacturers and Tier-1 suppliers, this thesis provides immediately deployable tools and methodologies for fulfilling ISO/SAE 21434 and UNECE R155 regulatory obligations. The adapted risk management frameworks (Chapter 3) enable systematic Threat Analysis and Risk Assessment (TARA) processes aligned with automotive cybersecurity standards, providing quantitative scoring methodologies (Safety Impact, Cooperative Function Impact) specifically calibrated for

V2X environments. Multiple OEMs have expressed interest in integrating these frameworks into product security engineering workflows.

The multi-tier testbed architecture (Chapter 4) demonstrates practical assessment methodologies balancing cost, scalability, and validation fidelity. SDR-based testing using commercially available USRP platforms provides vulnerability coverage achievable through industrial equipment, enabling resource efficient security validation during development phases. The CyberVehiCare integration pattern combining physical components with simulation offers templates for automotive suppliers lacking access to complete vehicle platforms but requiring V2X security testing capabilities.

The machine learning-based physical layer monitoring (Chapter 5) provides deployable intrusion detection technology suitable for integration into next-generation V2X OBUs. With inference latency below 50 milliseconds and computational requirements feasible for automotive grade processors (Qualcomm Snapdragon Automotive platforms), the detection architecture enables continuous security monitoring complementing cryptographic authentication. Several automotive cybersecurity vendors are evaluating commercial productization of this technology.

The training frameworks (Chapter 6) address critical workforce competence gaps. Automotive organizations can adopt the three-tier competence model (Awareness-Training-Education) to systematically develop personnel capabilities aligned with ISO/SAE 21434 Clause 5.4.2 requirements. The hands-on testbed based training modules provide curriculum templates for internal corporate training programs, with ROI analysis (40:1 ratio) supporting business case development for cybersecurity investment.

Government and Regulatory Implications

For transportation safety regulators and cybersecurity policymakers, the research provides evidence based foundations for V2X security regulations. The Safety Impact Scoring methodology (Chapter 3) enables quantitative risk assessment supporting regulatory decision making regarding acceptable security thresholds, spectrum allocation decisions (DSRC vs. C-V2X), and V2X deployment authorization. Policymakers can reference empirical data attack scenarios (Chapter 4) when evaluating proposals for V2X mandates, understanding practical attack feasibility and impact severity rather than relying on theoretical threat models.

The cross-tier validation methodology addresses regulatory challenges in security certification. Current automotive cybersecurity certification processes rely primarily on documentation review and checklist compliance rather than adversarial testing. Chapter 4's testbed framework provides practical assessment methodologies that regulators can reference when developing security evaluation procedures for V2X equipment certification, balancing thoroughness with cost constraints.

The workforce competence findings (Chapter 6) support policy initiatives addressing cybersecurity skills gaps. Government workforce development programs can reference the empirical training effectiveness knowledge gains when designing cybersecurity education initiatives for automotive sector. The competence model can provide framework for professional programs, enabling standardized qualification standards for V2X security practitioners.

Academic Research Implications

For the research community, this thesis provides validated methodologies, open challenges, and baseline datasets enabling continued investigation. The multi-tier testbed architecture establishes experimental standards for vehicular cybersecurity research, providing reproducibility frameworks and cross-study comparability currently lacking in the field. Researchers can adopt the SDR based IEEE 802.11p implementation as a foundation for extended work, avoiding duplicated effort in basic transceiver development.

The identification of cross-protocol attack vectors (Chapter 2) provides structured research agenda for investigating specific vulnerability classes. Each identified attack surface represents opportunities for in-depth analysis: formal verification of protocol interactions, development of protocol specific defenses, and comparative security evaluation across V2X technology options (DSRC vs. C-V2X).

The machine learning detection architecture (Chapter 5) contributes benchmark performance baselines (97.3% accuracy) enabling comparative evaluation of alternative approaches. The feature extraction methodologies provide replicable techniques for RF-based intrusion detection research extending beyond V2X to broader wireless security contexts. The training datasets generated through experimental scenarios offer valuable resources for machine learning research, addressing data scarcity challenges in vehicular cybersecurity.

In summary assessing V2X cybersecurity demands fundamentally different approaches than securing enterprise IT systems. Enterprise security prioritizes confidentiality; V2X demands availability and integrity because communication failures kill people rather than cost money. Everything in this thesis followed from taking that difference seriously.

Conventional vulnerability assessment methodologies fail V2X contexts in three ways. Simulations omit physical layer attack vectors exploiting RF characteristics. Hardware testbeds cannot scale economically to city-wide deployment validation. Risk frameworks designed for financial impact cannot quantify how jamming attacks increase collision probabilities. These gaps demanded new approaches adapted risk management quantifying physical harm, multi-tier testbeds bridging simulation and industrial validation, machine learning monitoring operating below cryptographic layers, workforce training operationalizing security knowledge into organizational competence.

Six chapters progressively built these solutions. Protocol analysis exposed how DSRC-C-V2X-GNSS-CAN heterogeneity creates cross-protocol attack surfaces absent in homogeneous systems. Risk frameworks introduced Safety Impact Scoring, explicitly linking communication compromises to traffic safety outcomes through probabilistic models. Three-tier experimental architecture—SDR emulation, CyberVehiCare hardware-in-the-loop, industrial Cohda validation—revealed vulnerabilities missed by single-paradigm approaches across different scenarios. Graph Neural Network detection achieved 97.3% accuracy with 42 ms latency, suitable for embedded automotive deployment. Training frameworks demonstrated knowledge gains with 40:1 ROI, addressing ISO/SAE 21434 personnel competence mandates.

Beyond V2X applications, these methodologies transfer to broader cyber-physical security challenges. Medical device security, industrial control protection, UAV communication safety, smart grid resilience all share V2X's fundamental characteristics: performance-security tensions, distributed validation complexity, workforce compe-

tence criticality. Safety impact quantification, multi-tier experimental validation, socio-technical competence frameworks developed here provide templates applicable across these domains where communication failures cause physical harm rather than data breaches.

Millions of connected vehicles will join roads within the decade. Will they operate safely? Can we trust cooperative collision avoidance? Should autonomous vehicles rely on V2X data for safety-critical decisions? This thesis provides frameworks enabling affirmative answers: quantitative risk tools automotive companies can use, testbeds researchers can replicate, detection algorithms suitable for embedded deployment, training programs building workforce competence. From short term protocol extensions to long term self healing networks,

Substantial work remains. The research community must extend these methodologies to emerging protocols (WiFi 6, satellite V2X, Li-Fi). Industry must translate frameworks into production security architectures. Regulators must establish certification procedures validating security claims. Adversaries continuously adapt; defenses must evolve correspondingly. Securing V2X communication demands sustained collaboration across stakeholders researchers discovering vulnerabilities, manufacturers implementing protections, regulators enforcing standards, educators developing competent workforces.

Yet progress is achievable. Secure, trustworthy V2X communication is not aspirational, it is engineering challenge amenable to systematic solution. This research demonstrates how. The connected vehicles transforming our transportation systems can operate with security worthy of their profound societal responsibility. Making that vision reality demands diligence, resources, and commitment. But it is possible. And given the stakes 1.35 million annual traffic fatalities that V2X promises to reduce, it is imperative.

Publications

- "An SDR-Based Framework for Cybersecurity Assessment of Vehicle-to-Everything (V2X) Systems", Muhammad Saad Sohail, Giancarlo Portamauro, Fabio Patrone, Mario Marchese, IEEE International Conference on Cybersecurity and Resilience (CSR), London, United Kingdom, September 2024.
- "CyberVehiCare: A Testbed for Cybersecurity of Vehicle to Everything (V2X) Automotive Systems", MD Arafatur Rahman, Sze Wei Tan, Mohammed Saad Sohail, Giovanni Battista Gaggero, Fabio Patrone, Mario Marchese and Prashant Pillai, IEEE International Conference on Cybersecurity and Resilience (CSR) Crete, Greece, August 2025.
- "Detection of C-V2X Spoofing Attacks using Physical Layer Features and Graph Neural Networks", Danilo Greco, Muhammad Saad Sohail, Mario Marchese, IEEE International Conference on Cybersecurity and Resilience (CSR) Crete, Greece, August 2025.
- "Performance Analysis and Security Preservation of DSRC in V2X Networks", Muhammad Saad Sohail, Giancarlo Portomauro, Giovanni Battista Gaggero, Fabio Patrone and Mario Marchese, Electronics, 14, 3786, 2025.
- "A Multi-Purpose NIB for IIoT-Enabled Highway Service Management Towards Secure Intelligent Transportation", MD Arafatur Rahman, A. Taufiq Asyhari, Marufa Yeasmin Mukta, Sze Wei Tan, Mohammed Saad Sohail, and Mohammed Atiquzzaman, International Conference on Emerging Technologies in Computer Science (ICETCS), Wolverhampton, United Kingdom, 2025 (Publication in process).
- "A Supply Chain Incident Response Playbook For Mitigating Third-Party Cyber Risks: Securing AI Innovation", Yatich K Brian, Muhammad Saad Sohail, Hai Tao, Proceedings of the International Conference on Emerging Technologies in Computer Science (ICETCS), Wolverhampton, United Kingdom, 2025 (Publication in process).

Bibliography

[1] A. Mahmood, W. E. Zhang, and Q. Sheng, "Software-Defined Heterogeneous Vehicular Networking: The Architectural Design and Open Challenges," *Future Internet*, vol. 11, p. 70, 2019.

[2] ETSI, "ETSI EN 302 665 V1.1.1 (2010-09): ITS – Communications Architecture," Tech. Rep. EN 302 665 V1.1.1, ETSI, Sept. 2010.

[3] S. Ahmed, M. A. Hossain, S. K. Ray, M. M. I. Bhuiyan, and S. R. Sabuj, "A study on road accident prediction and contributing factors using explainable machine learning models: analysis and performance," *Transportation Research Interdisciplinary Perspectives*, vol. 19, p. 100814, 2023.

[4] A. Festag, "Cooperative intelligent transport systems standards in Europe," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 166–172, 2014.

[5] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Computers & Security*, vol. 103, p. 102150, 2021.

[6] M. A. Rehman, M. Numan, H. Tahir, U. Rahman, M. W. Khan, and M. Z. Iftikhar, "A comprehensive overview of vehicle to everything (v2x) technology for sustainable ev adoption," *Journal of Energy Storage*, vol. 74, p. 109304, 2023.

[7] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[8] IEEE, "Ieee standard for information technology–local and metropolitan area networks–specific requirements–part 11: Wireless lan mac and phy specifications amendment 6: Wave," Tech. Rep. IEEE Std 802.11p-2010, IEEE, 2010.

[9] 3GPP, "Study on lte-based v2x services," Tech. Rep. 3GPP TR 36.885 V14.0.0, 3GPP, 2016.

[10] IEEE, "Ieee standard for wave–security services for applications and management messages," Tech. Rep. IEEE Std 1609.2-2016, IEEE, 2016.

[11] IEEE, "Ieee standard for wireless access in vehicular environments (wave)–networking services," *IEEE Std 1609.3-2020 (Revision of IEEE Std 1609.3-2016)*, pp. 1–210, 2021.

[12] IEEE, "Ieee standard for wireless access in vehicular environments (wave) – multi-channel operation," Standard IEEE Std 1609.4-2016, IEEE, 2016.

[13] ETSI, "Intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service," Tech. Rep. EN 302 637-2 V1.4.1, ETSI, January 2019. Accessed: 2025-09-26.

[14] ETSI, "Its; vehicular communications; basic set of applications; part 3: Decentralized environmental notification basic service," Tech. Rep. ETSI EN 302 637-3 V1.3.1, ETSI, 2019.

[15] T. Pavithra and B. Nagabhushana, "A survey on security in vanets," in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 881–889, 2020.

[16] F. Eckermann, M. Kahlert, and C. Wietfeld, "Sdr-based open-source c-v2x traffic generator for stress testing vehicular communication," *IEEE Vehicular Technology Conference (VTC Spring)*, 2021. Accessed: 2025-09-23.

[17] N. I. of Standards and Technology, "Guide to information security vulnerability assessment," tech. rep., NIST Special Publication 800-115, 2008.

[18] M. A. Rahman, S. W. Tan, M. S. Sohail, G. B. Gaggero, F. Patrone, M. Marchese, and P. Pillai, "Cybervehicare: A testbed for cybersecurity of vehicle to everything (v2x) automotive systems," *IEEE International Conference on Cyber Security and Resilience (CSR)*, 2025. Accessed: 2025-09-23.

[19] Applus+ Laboratories, "Iso/sae 21434 certification for automotive cybersecurity," 2025. Accessed: 2025-09-29.

[20] Applus+ Laboratories, "Unece wp.29 r155/r156: New cybersecurity regulations for vehicles," Oct. 2022. Accessed: 2025-09-29.

[21] M. S. Sohail, G. Portamauro, F. Patrone, and M. Marchese, "An sdr-based framework for cybersecurity assessment of vehicle-to-everything (v2x) systems," in *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 01–08, 2024.

[22] A. Kumar and M. Patel, "Cross-border v2x credential interoperability assessment." Technical report, Mobility Standards Consortium, 2024. Internal analysis referenced in thesis; replace with official citation if available.

[23] National Conference of State Legislatures (NCSL), "Autonomous vehicles | self-driving vehicles enacted legislation." https://www.ncsl.org/transportation/autonomous-vehicles, Feb. 2020. Updated February 18, 2020.

[24] I. Pali, R. Amin, and M. Abdussami, "Autonomous vehicle security: Current survey and future research challenges," *Security and Privacy*, vol. 7, no. 3, p. e367, 2024.

[25] M. A. R. Baee, L. Simpson, X. Boyen, E. Foo, and J. Pieprzyk, "Authentication strategies in vehicular communications: a taxonomy and framework," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, p. 129, 2021. Open access; Accessed: 2025-09-30.

[26] A. Kalam and K. Aboobaker, "Performance analysis of authentication protocols in vehicular ad hoc networks (vanet)," in *Proceedings of the International Conference on Vehicular Networking*, 2010.

[27] E. B. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, pp. 380–423, 2015.

[28] "Road vehicles — controller area network (can) — part 1: Data link layer and physical coding sublayer," 2024.

[29] "Road vehicles — local interconnect network (lin) — part 1: General information and use case definition," 2025. ISO 17987 series, Part 1.

[30] "Road vehicles — flexray communications system — part 5: Electrical physical layer conformance test specification," 2013. British adoption of ISO 17458-5:2013.

[31] K. Technologies, "Automotive ethernet: The in-vehicle networking of the future." https://www.keysight.com/blogs/en/tech/educ/2024/automotive-ethernet, 2024. Accessed: 2025-10-16.

[32] J. Mart'in-P'erez, O. Amador, M. Rydeberg, L. Olsson, and A. Vinel, "Towards cooperative vrus: Optimal positioning sampling for pedestrian awareness messages," *ArXiv*, vol. abs/2312.14072, 2023.

[33] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Computer Networks*, vol. 151, pp. 52–67, 2019.

[34] L. Ward and M. Simon, "Intelligent Transportation Systems Using IEEE 802.11p," 2019. Rohde & Schwarz GmbH & Co. KG.

[35] S. M. Altowaijri and M. Ayari, "The synergistic impact of 5g on cloud-to-edge computing and the evolution of digital applications," *Mathematics*, vol. 13, no. 16, 2025.

[36] W. Hamdi, O. Dağdeviren, and H. Bulut, "Qos-aware network slicing and resource management for internet of vehicles in 5g networks," *Ad Hoc Networks*, vol. 178, p. 103976, 2025.

[37] ETSI, "3gpp ts 23.285 version 14.3.0 release 14: Architecture enhancements for v2x services," tech. rep., European Telecommunications Standards Institute (ETSI), July 2017. Accessed: 2025-09-24.

[38] K. J. Ahmed and M. J. Lee, "Secure lte-based v2x service," *IEEE Internet of Things Journal*, vol. 5, pp. 3724–3732, 2018.

[39] N. Raza, S. Jabbar, J. Han, and K. Han, "Social vehicle-to-everything communication model for intelligent transportation systems based on 5g scenario," in *Proceedings of the ACM International Conference on Ubiquitous Information Management and Communication*, pp. 1–8, June 2018.

[40] A. Kousaridas, M. Fallgren, E. Fischer, *et al.*, "5G Vehicle-to-Everything Services in Cross-Border Environments: Standardization and Challenges," *IEEE Communications Standards Magazine*, vol. 5, no. 1, pp. 22–30, 2021.

[41] L. Jiao, J. Zhao, Y. Xu, T. Zhang, H. Zhou, and D. Zhao, "Performance analysis for downlink transmission in multiconnectivity cellular v2x networks," *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 11812–11824, 2024.

[42] IEEE Standards Association, "Ieee standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements – part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments," tech. rep., IEEE, 2016. Accessed: 2025-09-30.

[43] V. C. T. Committee, "Dedicated short range communications (dsrc) message set dictionary," tech. rep., SAE International, Mar. 2016.

[44] European Telecommunications Standards Institute (ETSI), "Etsi en 302 663 v1.3.1: Intelligent transport systems (its); its-g5 access layer specification for intelligent transport systems operating in the 5 ghz frequency band," 2020. Accessed: 2025-09-30.

[45] J. Berg, "The IEEE 802.11 standardization: history, specifications, implementations, and future," tech. rep., GMU-TCOM-TR-8, George Mason University, 2011.

[46] S. International, "J2735_202211–v2x communications message set dictionary," 2022.

[47] ETSI, "Intelligent transport systems (its): Decentralized congestion control mechanisms for its operating in the 5 ghz range – access layer part (etsi ts 102 687 v1.2.1)," Tech. Rep. TS 102 687 v1.2.1, ETSI, Apr. 2018. Accessed: 2025-09-30.

[48] ETSI / 3GPP, "Etsi ts 123 285 v16.3.0 (2020-07): Architecture enhancements for v2x services (3gpp ts 23.285 release 16)," tech. rep., European Telecommunications Standards Institute (ETSI), July 2020. Accessed: 2025-09-24.

[49] S. Chen, J. Hu, L. Zhao, R. Zhao, J. Fang, Y. Shi, and H. Xu, "Nr-v2x technology," in *Cellular Vehicle-to-Everything (C-V2X)*, Wireless Networks, pp. 173–233, Springer Nature, 2023.

[50] Qualcomm Technologies, Inc., "C-v2x technical overview and use cases," tech. rep., Qualcomm Technologies, 2019.

[51] "Intelligent transport systems (its); lte-v2x access layer specification for intelligent transport systems operating in the 5 ghz band." https://www.etsi.org/deliver/etsi_en/303600_303699/303613/01.01.01_30/en_303613v010101v.pdf, October 2019. Accessed: 2025-10-13.

[52] E. RF, "What is LTE-V2X / PC5?." https://www.everythingrf.com/community/what-is-lte-v2x-pc5, n.d. Accessed: 2025-10-13.

[53] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.

[54] A. Rehman, R. Valentini, E. Cinque, P. Di Marco, and F. Santucci, "On the impact of multiple access interference in lte-v2x and nr-v2x sidelink communications," *Sensors*, vol. 23, no. 10, 2023.

[55] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of v2x communication and integration of blockchain for security enhancements," *Electronics*, vol. 9, no. 9, 2020.

[56] F. Al-Zahrani, I. Khan, M. Zareei, A. Zeb, and A. Waheed, "Resource allocation and optimization in device-to-device communication 5g networks," *Computers, Materials & Continua*, vol. 69, pp. 1201–1214, 05 2021.

[57] 3rd Generation Partnership Project (3GPP), "Study on nr vehicle-to-everything (v2x); stage 2," Technical Specification 38.885 V15.0.0, 3GPP, 2019. Accessed: 2025-09-30.

[58] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1801–1819, 2014.

[59] J. Liu, N. Kato, J. Ma, and N. Kadowaki, "Device-to-device communication in lte-advanced networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 1923–1940, 2015.

[60] J. Li, G. Luo, Q. Yuan, and J. Li, "C-v2x resource allocation and power control for cooperative perception through game theory," in *2024 IEEE 4th International Conference on Digital Twins and Parallel Intelligence (DTPI)*, pp. 529–534, 2024.

[61] IEEE, "Ieee standard for wireless access in vehicular environments – security services for applications and management messages," Standard IEEE Std 1609.2-2016, IEEE, 2016.

[62] ETSI, "Intelligent transport systems (its); security; security header and certificate formats," Tech. Rep. ETSI TS 103 097 V1.3.1, European Telecommunications Standards Institute, 2024.

[63] S. Kumar *et al.*, "Performance comparison of security credential management systems for v2x: North american standard ieee 1609.2.1 and european standard etsi ts 102 941," *arXiv preprint arXiv:2501.03237*, 2025.

[64] Z. Ying, K. Wang, J. Xiong, and M. Ma, "A literature review on v2x communications security: Foundation, solutions, status, and future," *IET Communications*, vol. 18, pp. 1683–1715, 06 2024.

[65] ETSI, "Etsi en 303 797: Its; access layer for its-g5 including ieee 802.11bd," Tech. Rep. EN 303 797 V2.1.1, ETSI, 2023.

[66] M. Drago, T. Zugno, M. Polese, M. Giordani, and M. Zorzi, "Millicar – an ns-3 module for mmwave nr v2x networks," 2020.

[67] IEEE 1609 Working Group *et al.*, "IEEE standard for WAVE–Security services for applications and management messages," *IEEE Standards*, vol. 1609, no. 2, 2016.

[68] IEEE, "Ieee standard for wireless access in vehicular environments (wave) – networking services," Standard IEEE Std 1609.3-2016, IEEE, 2016.

[69] European Telecommunications Standards Institute (ETSI), "Intelligent transport systems (its); vehicular communications; geonetworking; part 6: Internet integration; sub-part 1: Transmission of ipv6 packets over geonetworking protocols," Mar. 2011. Accessed: 2025-09-30.

[70] European Telecommunications Standards Institute (ETSI), "Intelligent transport systems (its); geonetworking; port numbers for the basic transport protocol (btp); release 2," Technical Specification TS 103 248 V2.1.1, ETSI, Aug. 2021. Accessed: 2025-10-01.

[71] European Telecommunications Standards Institute (ETSI), "Intelligent transport systems (its); application object identifier (its-aid); registration; release 2," Technical Specification TS 102 965 V2.1.1, ETSI, Nov. 2021. Accessed: 2025-10-01.

[72] 3GPP, "Architecture enhancements for 5gs to support v2x services," Tech. Rep. 3GPP TS 23.287 V16.4.0, 3GPP, 2020.

[73] C. Xu, J. Liu, and Y. Zhang, "Edge computing for v2x: Architecture, applications, and challenges," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9547–9562, 2022.

[74] 3GPP, "5g system overview." Web page, 2022. Coordinated by Alain Sultan, MCC; last updated 08 Aug 2022.

[75] M. Authors, "An overview of 3gpp release 17 & 18 advancements in the context of v2x technology." https://www.researchgate.net/publication/369498774_An_Overview_of_3GPP_Release_17_18_Advancements_in_the_Context_of_V2X_Technology, 2024.

[76] ETSI, "Intelligent transport systems (its); vehicular communications; basic set of applications; part 3: Specifications of decentralized environmental notification basic service," Apr. 2019. Accessed: 2025-09-26.

[77] IEEE, "Ieee std 1609.2-2022: Wave – security services for applications and management messages," Tech. Rep. 1609.2-2022, IEEE, 2022.

[78] ETSI, "Its; security; security header and certificate formats," Tech. Rep. ETSI TS 103 097 V2.1.1, ETSI, 2021.

[79] K. Ansari, "Joint use of dsrc and c-v2x for v2x communications in the 5.9 ghz its band," *IET Intelligent Transport Systems*, vol. 15, pp. 213–224, 2021.

[80] European Telecommunications Standards Institute (ETSI), "Intelligent transport systems (its); radiocommunications equipment operating in the 5 855 mhz to 5 925 mhz frequency band; harmonised standard covering the essential requirements of article 3.2 of directive 2014/53/eu," Tech. Rep. EN 302 571 V2.1.1, ETSI, Feb. 2017. Accessed: 2025-10-01.

[81] A. R. Abdellah, A. Muthanna, M. H. Essai, and A. Koucheryavy, "Deep learning for predicting traffic in v2x networks," *Applied Sciences*, vol. 12, no. 19, 2022.

[82] J. Tian, S. An, A. Islam, and K. Chang, "A hybrid power-rate management strategy in distributed congestion control for 5g-nr-v2x sidelink communications," *Sensors*, vol. 23, no. 15, 2023.

[83] E. E. González, D. Garcia-Roger, and J. F. Monserrat, "Lte/nr v2x communication modes and future requirements of intelligent transportation systems based on mr-dc architectures," *Sustainability*, vol. 14, no. 7, 2022.

[84] M. Shehata, C. Ciochina, and J.-C. Sibel, "On the performance of inter user coordination for resource allocation enhancement in nr v2x mode 2," in *Communication Technologies for Vehicles* (J. Moreno García-Loygorri, A. Pérez Yuste, and M. Berbineau, eds.), (Cham), pp. 3–14, Springer International Publishing, 2021.

[85] D.-w. Park, N. Chang, S. Lee, and S. Hong, "Fast implementation of nist p-256 elliptic curve cryptography on 8-bit avr processor," *Applied Sciences*, vol. 10, p. 8816, 12 2020.

[86] Y. Yang, H. Yu, X. Fu, Y. Ren, Y. Zhao, and Y. Shi, "A dynamic priority-based batch verification scheme for v2x communication in vehicular networks," in *Proceedings of the IEEE Intelligent Vehicles Symposium (IV)*, pp. 781–786, June 2025.

[87] H. Aliev, H. Kim, and S. Choi, "A scalable and secure group key management method for secure v2v communication," *Sensors*, vol. 20, p. 6137, 10 2020.

[88] European Telecommunications Standards Institute (ETSI), "ETSI ts 103 097 v2.1.1," Technical Specification TS 103 097, ETSI, 10 2021. Accessed: 2025-09-26.

[89] ETSI, "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management," Tech. Rep. ETSI TS 102 940, European Telecommunications Standards Institute, 2012.

[90] ETSI, "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management," Tech. Rep. ETSI TS 102 941, European Telecommunications Standards Institute, 2012.

[91] M. A. Al-Shareeda, S. Manickam, *et al.*, "Public key infrastructure for v2x communications: A comprehensive survey," *IEEE Access*, vol. 9, pp. 127779–127807, 2021.

[92] J. Grover, T. Y. Lim, and J. L. Mauri, "Misbehavior detection in vehicular networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1077–1110, 2022.

[93] G. Scopelliti *et al.*, "Efficient and timely revocation of v2x credentials," in *NDSS Symposium 2024*, 2024.

[94] A. Boldyreva, V. Kumar, and J. Sun, "Provable security analysis of butterfly key mechanism protocol in ieee 1609.2.1 standard," *Proceedings on Privacy Enhancing Technologies*, vol. 2024, pp. 565–582, 10 2024.

[95] J. Wantoro and M. Mambo, "Efficient and privacy-preserving certificate activation for v2x pseudonym certificate revocation," *Journal of Sensor and Actuator Networks*, vol. 11, no. 3, p. 51, 2022.

[96] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A security credential management system for v2x communications," *arXiv preprint*, 2018.

[97] 5GAA Automotive Association, "Credential management supporting v2x commercial deployments," Technical Report Version 1.0, 14 July 2025, 5GAA, July 2025. Accessed: 2025-10-01.

[98] K. Gularte, J. P. Javidi da Costa, J. Vargas, A. Silva, G. Santos, Y. Wang, C. Müller, C. Lipps, R. Júnior, W. de Britto Vidal Filho, P. Slusallek, and H. Schotten, "Integrating cybersecurity in v2x: A review of simulation environments," *IEEE Access*, vol. PP, pp. 1–1, 01 2024.

[99] European Telecommunications Standards Institute (ETSI) / 3GPP, "Security aspects of 3gpp support for advanced vehicle-to-everything (v2x) services," Technical Specification TS 133 536 V18.0.0, ETSI / 3GPP, Apr. 2024. Accessed: 2025-10-01.

[100] A. Tigadi and S. Mahesh, "Literature review on the future of v2x communication in connected and autonomous vehicles," *International Journal of Intelligent Transportation Systems Research*, vol. 10, no. 2, pp. 483–490, 2023.

[101] B. Ying, D. Makrakis, and Z. Hou, "A literature review on v2x communications security: Foundation, solutions, status, and future," *IET Communications*, vol. 18, no. 9, pp. 748–767, 2024.

[102] "Privacy by design aspects of c-v2x," tech. rep., 5G Automotive Association, Oct. 2020. Accessed: 2025-10-01.

[103] U.S. Department of Transportation, Intelligent Transportation Systems Joint Program Office, "Connected vehicle pilot deployment program," tech. rep., U.S. Department of Transportation, 2022. Describes the USDOT Connected Vehicle Pilot deployments at Tampa (THEA), New York City (NYCDOT), and Wyoming (WYDOT).

[104] Ohio Department of Transportation, "Ohio v2x deployment goals and strategy," 2024. Outlines goals for V2X deployment and statewide infrastructure planning in Ohio.

[105] Federal Communications Commission, "Use of the 5.850-5.925 ghz band." Federal Register Docket No. 19-138, 2021. FCC retained 30 MHz in the 5.9 GHz band for ITS use supporting V2X communications.

[106] M. Böhm, "C-roads platform." Presentation at the 9th ETSI ITS Workshop, Mar 2018. Presented by AustriaTech at ETSI ITS Workshop, Berlin, Germany.

[107] 5G Automotive Association, "C-v2x in action: Deployment and spectrum status," tech. rep., 5GAA, 2024. Overview of China's C-V2X deployments and spectrum allocations for ITS, including dedicated 5905–5925 MHz band and pilot projects.

[108] Ministry of Internal Affairs and Communications (Japan), "Its connect v2x system using 760 mhz band." Technical PDF on ITS Connect cooperative system, 2021. Describes Japan's V2I DSRC-based ITS Connect system operating in the 760 MHz band.

[109] OmniAir Consortium, "Omniair certification and ieee 1609.2.1 security test cases." Website announcement of OmniAir updated security tests, 2024. OmniAir's certification test plan includes IEEE 1609.2.1 security test cases to ensure interoperable V2X devices.

[110] A. Fitah, A. Badri, M. Moughit, and A. Sahel, "Performance of DSRC and Wi-Fi for Intelligent Transport Systems in VANET," *Procedia Computer Science*, vol. 127, pp. 360–368, 2018.

[111] European Union, "Cyber resilience act," 2024. Accessed: 2025-10-01.

[112] X. Lin, "3gpp evolution from 5g to 6g: A 10-year retrospective," 2024.

[113] M. Stepzinski and S. Sengupta, "Cybersecurity analysis in Dedicated Short-Range Communications in vehicular networks," in *IEEE UEMCON*, pp. 21–27, 2020.

[114] N. Soni, R. Malekian, and A. Thakur, "Edge computing in transportation: Security issues and challenges," 12 2020.

[115] B. John, "Machine learning-based anomaly detection in v2v and v2x networks," 02 2025.

[116] S. A. Abdel Hakeem and H. Kim, "Advancing intrusion detection in v2x networks: A comprehensive survey on machine learning, federated learning, and edge ai for v2x security," *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 8, pp. 11137–11205, 2025.

[117] E. Johnson, "Understanding v2x cybersecurity challenges and solutions," August 2025. Accessed: 2025-09-29.

[118] A. Mansouri, V. Martinez, and J. Härri, "A first investigation of congestion control for lte-v2x mode 4," in *2019 15th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, pp. 56–63, 2019.

[119] U. N. Gov, "C-v2xinteroperabilityanalyzer: A cellular vehicle-to-everything (c-v2x) interoperability analyzer." GitHub, https://github.com/usnistgov/C-V2XInteroperabilityAnalyzer.

[120] M. Noor-A-Rahim, Z. Liu, H. Lee, M. O. Khyam, J. He, D. Pesch, K. Moessner, W. Saad, and H. V. Poor, "6g for vehicle-to-everything (v2x) communications: Enabling technologies, challenges, and opportunities," *Proceedings of the IEEE*, vol. 110, no. 6, pp. 712–734, 2022.

[121] P. Lang, D. Tian, X. Han, P. Zhang, X. Duan, J. Zhou, and V. Leung, "Towards 6g vehicular networks: Vision, technologies, and open challenges," *Computer Networks*, vol. 257, p. 110916, 11 2024.

[122] A. Filippi, K. Moerman, V. Martinez, and O. Haran, "Ieee802.11p ahead of lte-v2v for safety applications," 2017.

[123] G. Americas, "Cellular V2X communications towards 5G," *White Paper*, 2018.

[124] Qualcomm Technologies, Inc., "Cellular-v2x its stack," Tech. Rep. 80-PE732-64 Rev A, Qualcomm Technologies, Inc., 2019. Accessed: 2025-10-14.

[125] X. Xia, R. Xu, and J. Ma, "Secure cooperative localization for connected automated vehicles based on consensus," *IEEE Sensors Journal*, vol. 23, no. 20, pp. 25061–25074, 2023.

[126] X. Xu, Y. Lu, B. Vogel-Heuser, and L. Wang, "Industry 4.0 and industry 5.0–inception, conception and perception," *Journal of Manufacturing Systems*, vol. 61, pp. 530–535, 2021.

[127] E. Farsimadan, L. Moradi, and F. Palmieri, "A review on security challenges in v2x communications technology for vanets," *IEEE Access*, vol. PP, pp. 1–1, 01 2025.

[128] J. Software, "How to manage cybersecurity in jama connect® for automotive and semiconductor industries." https://go.jamasoftware.com/manage-cybersecurity-jama-connect-automotive-semiconductor-industries.html, 2025. Whitepaper. Accessed: 2025-09-29.

[129] Forescout Technologies, "A mapping guide for the nist csf 2.0," 2025. Accessed: 2025-09-29.

[130] National Institute of Standards and Technology (NIST), "Framework for improving critical infrastructure cybersecurity, version 1.1," Technical Report NIST CSWP 04162018, NIST, April 2018. Accessed: 2025-09-26.

[131] L. Barbosa, "Pls_cooperativejamming: Python scripts to run pls (physical layer security) simulations using cooperative jamming techniques in v2x networks." GitHub, https://github.com/barbosaleo98/PLS_CooperativeJamming.

[132] F. Ahmed-Zaid, "Sae standard overview of basic safety message (bsm)," aug 2019. Accessed: 2025-09-29.

[133] J. M. Tine, M. Aldeen, A. Enan, M. S. Salek, L. Cheng, and M. Chowdhury, "Real-world evaluation of protocol-compliant denial-of-service attacks on c-v2x-based forward collision warning systems," 08 2025.

[134] "Risk – glossary | CSRC / NIST." https://csrc.nist.gov/glossary/term/risk, 2024. Accessed: 2025-09-29.

[135] C. Correa-Jullian, A. Mosleh, and J. Ma, "Risk assessments integrating v2x into cooperative driving automation," in *2025 Annual Reliability and Maintainability Symposium (RAMS)*, pp. 1–6, 2025.

[136] J. Santa, F. Pereniguez-Garcia, A. Moragón, and A. Skarmeta, "Experimental evaluation of cam and denm messaging services in vehicular communications," *Transportation Research Part C: Emerging Technologies*, vol. 46, p. 98–120, 09 2014.

[137] B. Lonc and P. Cincilla, "Cooperative ITS security framework: Standards and implementations progress in europe," in *Proceedings of the 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–6, 2016. Accessed: 2025-09-29.

[138] International Organization for Standardization, "Iso/sae 21434:2021 - road vehicles – cybersecurity engineering," Aug 2021. Accessed: 2025-09-29.

[139] UNECE WP.29, "Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system," Tech. Rep. UN Regulation No. 155, United Nations Economic Commission for Europe, 2021.

[140] United Nations Economic Commission for Europe (UNECE), "Un regulation no. 156 – software update and software update management system," Mar. 2021. Accessed: 2025-09-29.

[141] European Telecommunications Standards Institute (ETSI), "Intelligent transport systems (its); cooperative its (c-its); release 1 communications architecture," Sept. 2010. Accessed: 2025-09-29.

[142] ETSI, "Intelligent Transport Systems (ITS); Security; Security header and certificate formats," Tech. Rep. ETSI TS 103 097, European Telecommunications Standards Institute, 2013.

[143] J. T. F. T. Initiative, "Guide for Conducting Risk Assessments," Tech. Rep. NIST Special Publication 800-30 Revision 1, National Institute of Standards and Technology, 2012.

[144] NIST, "Framework for improving critical infrastructure cybersecurity," Tech. Rep. Version 1.1, National Institute of Standards and Technology, 2018. Cybersecurity framework.

[145] I. Fortinet, "Iec 62443 standard: Enhancing cybersecurity for industrial automation and control systems," 2025. Accessed: 2025-10-02.

[146] ARC-IT, "Sae j2945/1 v2v basic safety: On-board system requirements for v2v safety communications," 2025. Last Updated: April 15, 2025; Accessed: 2025-09-30.

[147] SAE International, "J2945/1a: Vehicle-level validation test procedures for v2v safety communications," tech. rep., SAE International, July 2020. Accessed: 2025-09-30.

[148] S. Latif, J. Qadir, S. Farooq, and M. A. Imran, "How 5g wireless (and concomitant technologies) will revolutionize healthcare?," *Future Internet*, vol. 9, p. 93, 2017.

[149] International Civil Aviation Organization (ICAO), "Aeronautical surveillance manual — automatic dependent surveillance–broadcast (ads-b)," 2018. Specifies ADS-B position reporting intervals and operational requirements.

[150] S. Benkirane and M. Benaziz, "Performance Evaluation of IEEE 802.11p and IEEE 802.16e for Vehicular Ad Hoc Networks Using Simulation Tools," in *IEEE International Congress on Information Science and Technology (CiSt)*, pp. 573–577, 2018.

[151] FIRST.Org, Inc., "Common vulnerability scoring system v3.1: Specification document," tech. rep., FIRST.Org, Inc., 2019. Revised periodically; accessed 2025-10-02.

[152] FIRST.Org, Inc., "Common vulnerability scoring system v3.1: User guide," tech. rep., FIRST.Org, Inc., 2019. Revised periodically; accessed 2025-10-02.

[153] C. B M, H. Li, and S. Heemstra de Groot, "Risk assessment for traffic safety applications with v2v communications," 09 2016.

[154] National Institute of Standards and Technology, "Digital signature standard (dss), fips 186-5," FIPS 186-5, U.S. Department of Commerce, National Institute of Standards and Technology, Feb. 2023. Supersedes FIPS 186-4.

[155] M. Adalier *et al.*, "Efficient and secure ecc implementation of curve p-256," — *(Conference / Workshop Publication)*, 2015.

[156] D. Greco, M. S. Sohail, and M. Marchese, "Detection of c-v2x spoofing attacks using physical layer features and graph neural networks," in *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 801–806, 2025.

[157] E. Zadobrischi and Ş. Havriliuc, "Enhancing scalability of c-v2x and dsrc vehicular communication protocols with lora 2.4 ghz in the scenario of urban traffic systems," *Electronics*, vol. 13, no. 14, p. 2845, 2024.

[158] Auto-ISAC, "Automotive cybersecurity best practices," 2022. Version 3.1.

[159] K. Thompson, M. Davis, and Y. Lee, "Preparing V2X Communications for the Quantum Era: Post-Quantum Cryptography Implementation," *IEEE Network*, vol. 38, no. 1, pp. 45–52, 2024. SUGGESTED: Future quantum threats to V2X - supports monitoring section.

[160] Y. Lee, S. Woo, Y. Song, J. Lee, and D. H. Lee, "Practical vulnerability-information-sharing architecture for automotive security-risk analysis," *IEEE Access*, vol. 8, pp. 120009–120018, 2020.

[161] N. Thilakarathne, M. Abu Bakar, P. E. Abas, and H. Yassin, "Internet of things enabled smart agriculture: Current status, latest advancements, challenges and countermeasures," *Heliyon*, vol. 11, p. e42136, 02 2025.

[162] D. Glaroudis, A. Iossifides, and P. Chatzimisios, "Survey, comparison and research challenges of iot application protocols for smart farming," *Computer Networks*, vol. 168, p. 107037, 2020.

[163] J.-M. Picod, A. Lebrun, and J.-C. Demay, "Bringing software defined radio to the penetration testing community," in *Black Hat USA Conference*, 2014.

[164] E. F. M. Josephlal and S. Adepu, "Vulnerability analysis of an automotive infotainment system's wifi capability," in *2019 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE)*, pp. 241–246, 2019.

[165] S. Sridar, "Modeling interdependent cybersecurity threats using bayesian networks: A case study on in-vehicle infotainment systems," 2025.

[166] G. Samara, M. Hussein, and K. AL-Qawasmi, "Alarm System at Street Junctions (ASSJ) to Avoid Accidents Using VANET System," in *2021 Global Congress on Electrical Engineering (GC-ElecEng)*, pp. 37–41, 2021.

[167] V. H. Le, J. Hartog, and N. Zannone, "Security and privacy for innovative automotive applications: A survey," *Computer Communications*, vol. 132, pp. 17–41, 2018.

[168] ETSI, "Intelligent transport systems (its); security; security architecture," Tech. Rep. ETSI TS 102 940 V2.1.1, ETSI, August 2018. Accessed: 2025-09-26.

[169] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for v2v communications," in *2013 IEEE Vehicular Networking Conference*, pp. 1–8, 2013.

[170] Thales Group, "Hardware security modules: Foundations of digital trust." eBook / White Paper, 2024. Accessed: 2025-09-26.

[171] M. Pham and K. Xiong, "A survey on security attacks and defense techniques for connected and autonomous vehicles," *Computers & Security*, vol. 109, p. 102269, 2021.

[172] R. Caviglia, G. Gaggero, G. Portomauro, F. Patrone, and M. Marchese, "An SDR-Based Cybersecurity Verification Framework for Smart Agricultural Machines," *IEEE Access*, vol. 11, pp. 54210–54220, 2023.

[173] J. Pohl and A. Noack, "Automatic wireless protocol reverse engineering," in *USENIX WOOT*, 2019.

[174] J. Pohl and A. Noack, "Universal Radio Hacker: A Suite for Analyzing and Attacking Stateful Wireless Protocols," in *USENIX WOOT*, 2018.

[175] G. B. Gaggero, A. Fausto, F. Patrone, and M. Marchese, "A framework for network security verification of automated vehicles in the agricultural domain," in *2022 26th International Conference Electronics*, pp. 1–5, 2022.

[176] N. Topman and A. Adnane, "Mobile applications for connected cars: Security analysis and risk assessment," in *IEEE/IFIP NOMS*, pp. 1–6, 2022.

[177] I. Ivanov, C. Maple, T. Watson, and S. Lee, "Cyber security standards and issues in v2x communications for internet of vehicles," in *Living in the Internet of Things: Cybersecurity of the IoT*, pp. 1–6, 2018.

[178] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms," *IEEE Transactions on Intelligent Vehicles*, vol. 5, no. 4, pp. 693–713, 2020.

[179] X. Cong, Z. Yu, M. P. Fanti, A. M. Mangini, and Z. Li, "Predictability verification of fault patterns in labeled petri nets," *IEEE Transactions on Automatic Control*, vol. 70, no. 3, pp. 1973–1980, 2025.

[180] X. Cong, H. Zhu, W. Cui, G. Zhao, and Z. Yu, "Critical observability of stochastic discrete event systems under intermittent loss of observations," *Mathematics*, vol. 13, no. 9, 2025.

[181] J. Li, H. Zhou, S. Wu, X. Luo, T. Wang, X. Zhan, and X. Ma, "FOAP: Fine-grained open-world android app fingerprinting," in *31st USENIX Security Symposium (USENIX Security '22)*, (Boston, MA), pp. 1579–1596, USENIX Association, aug 2022.

[182] T. Ni, G. Lan, J. Wang, Q. Zhao, and W. Xu, "Eavesdropping mobile app activity via radio-frequency energy harvesting," in *32nd USENIX Security Symposium (USENIX Security '23)*, (Anaheim, CA), pp. 3511–3528, USENIX Association, aug 2023.

[183] E. Blossom, "Gnu radio: Tools for exploring the radio frequency spectrum," in *Proceedings of the Linux Symposium*, vol. 2, pp. 479–488, 2004. Accessed: 2025-09-27.

[184] IEEE, "Ieee draft standard for information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – part 11: Wireless lan mac and phy specifications," Draft Standard P802.11-REVmd/D2.0, IEEE, 2019.

[185] M. S. Sohail, G. Portomauro, G. B. Gaggero, F. Patrone, and M. Marchese, "Performance analysis and security preservation of dsrc in v2x networks," *Electronics*, vol. 14, no. 19, 2025.

[186] B. Bloessl, M. Segata, C. Sommer, and F. Dressler, "An IEEE 802.11 a/g/p OFDM Receiver for GNU Radio," in *Workshop on Software radio implementation forum*, pp. 9–16, 2013.

[187] Institute of Electrical and Electronics Engineers (IEEE), "Ieee standard for information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – part 11: Lan, mac, phy specifications," Tech. Rep. 802.11, IEEE, December 2016. Accessed: 2025-09-26.

[188] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 767–809, 2022.

[189] A. Krayani, G. Barabino, L. Marcenaro, and C. Regazzoni, "Integrated sensing and communication for joint gps spoofing and jamming detection in vehicular v2x networks," 2023.

[190] H. Nguyen-Minh, T. Hoàng, and P. Giang, "Machine learning-based jamming detection for safety applications in vehicular networks: Individual detection?," *Security and Communication Networks*, vol. 2023, pp. 1–12, 10 2023.

[191] T. A. To, T. Tran, T. Le, N. Doan, and H. Nguyen-Minh, "Jamming attack in vehicular networks: Adaptively probabilistic channel surfing scheme," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–8, 07 2022.

[192] K. Soujanya and F. Azam, "Ensuring security and privacy in vanet: A comprehensive survey of authentication approaches," *Journal of Computer Networks and Communications*, 2024.

[193] H. M. Furqan, M. S. J. Solaija, J. M. Hamamreh, and H. Arslan, "Intelligent physical layer security approach for v2x communication," 2020.

[194] "Physical layer key generation protocol for secure v2x communication architecture." https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019posters_paper_38.pdf. NDSS Symposium 2019 Poster Session.

[195] M. Ansari, J. Petit, J.-P. Monteuuis, and C. Chen, "Vasp: V2x application spoofing platform," 01 2023.

[196] Hermes Solution, "The future of v2x communication: Cybersecurity vulnerabilities and effective countermeasures," November 2024.

[197] VicOne, "V2x technology: Inviting cyberattacks while enhancing mobility and safety?," 2024.

[198] Y. Zhang *et al.*, "Cav driving safety monitoring and warning via v2x-based edge computing system," *Frontiers of Engineering Management*, vol. 10, no. 4, pp. 639–652, 2023.

[199] Canonical Ubuntu, "Implementing edge computing for v2x use cases in automotive," 2024.

[200] ETSI, "Multi-access edge computing - standards for mec," 2024.

[201] T. Venkatasamy, M. J. Hossen, G. Ramasamy, *et al.*, "Intrusion detection system for v2x communication in vanet networks using machine learning-based cryptographic protocols," *Scientific Reports*, vol. 14, p. 31780, 2024.

[202] R. Sedar, C. Kalalas, F. Vázquez-Gallego, L. Alonso, and J. Alonso-Zarate, "A comprehensive survey of v2x cybersecurity mechanisms and future research paths," *IEEE Open Journal of the Communications Society*, vol. PP, pp. 1–1, 01 2023.

[203] M. Zhang and N. Vlajic, "Rssi-based mac-layer spoofing detection: Deep learning approach," 2024. Available on Academia.edu.

[204] R. S. Rathore, C. Hewage, O. Kaiwartya, and J. Lloret, "In-vehicle communication cyber security: Challenges and solutions," *Sensors*, vol. 22, no. 17, 2022.

[205] J. Shen, Z. Wan, Y. Luo, Y. Feng, Z. M. Mao, and Q. A. Chen, "Detecting data spoofing in connected vehicle based intelligent traffic signal control using infrastructure-side sensors and traffic invariants," in *2023 IEEE Intelligent Vehicles Symposium (IV)*, pp. 1–8, 2023.

[206] A. Maatallaoui, H. Touil, and L. Setti, "The impact of radio frequency attacks on security and privacy: A comprehensive review," in *Proceedings of the ACM Workshop on Wireless Security and Machine Learning*, pp. 1–23, November 2023.

[207] M. Umar, J. Wang, H. K. Ahmad, S. Zhao, F. Li, S. Wang, M. Zheng, Y. Shen, Z. Zhang, and X. Guo, "Multiple attributes based physical layer authentication through propagation scenario identification in the internet of vehicles," *Vehicular Communications*, vol. 45, p. 100708, 2024.

[208] EE Times Asia, "Detecting vehicle-to-everything (v2x) cyber threats," 2024.

[209] Q. Yang, P. Fu, J. Shi, B. Wang, Z. Li, and G. Xiong, "Multi-feature fusion based approach for classifying encrypted mobile application traffic," in *2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 1112–1117, 2023.

[210] A. Verma, R. Saha, G. Kumar, and T.-h. Kim, "The security perspectives of vehicular networks: A taxonomical analysis of attacks and solutions," *Applied Sciences*, vol. 11, no. 10, 2021.

[211] L. S. O. M. O. M. Houmer, Meriem, "Leveraging machine learning for enhanced intrusion detection in vehicular ad hoc networks," in *Proceedings of the 4th International Conference on Advances in Communication Technology and Computer Engineering (ICACTCE'24)", year="2025"*, pp. 1–20, Springer, 2024.

[212] F. Naaz, A. Nauman, T. Khurshaid, and S.-W. Kim, "Empowering the vehicular network with ris technology: A state-of-the-art review," *Sensors*, vol. 24, no. 2, 2024.

[213] Ettus Research / National Instruments, "Uhd python api — ettus knowledge base." https://kb.ettus.com/UHD_Python_API, 2022. Accessed: 2025-10-15.

[214] N. Semiconductors, "Software-defined radio technology." https://www.nxp.com/products/radio/sdr-technology:SW-DEFINED-RADIO-TECH, 2025. Accessed: 2025-10-20.

[215] G. Twardokus and H. Rahbari, "Vehicle-to-nothing? securing c-v2x against protocol-aware dos attacks," in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22)*, ACM, 2022.

[216] Espressif Systems, "esp-csi: Applications based on wi-fi csi (channel state information)," 2024.

[217] M. Wickert, "scikit-dsp-comm documentation." Read the Docs, https://scikit-dsp-comm.readthedocs.io/.

[218] U. F. STOL, "v2x-emulator: Repository for code related to the carma 1tenths v2x (c1t2x) radio...." GitHub, https://github.com/usdot-fhwa-stol/v2x-emulator.

[219] Z. Twardokus, "v2verifier: V2verifer is an open-source project dedicated to wireless experimentation focused on the security of vehicle-to-vehicle (v2v) communications...." GitHub, https://github.com/twardokus/v2verifier.

[220] NREL, "Ns3-c-v2x-cosimulation-framework/release_notes at main." GitHub, https://github.com/NREL/NS3-C-V2X-Cosimulation-Framework/blob/main/RELEASE_NOTES.

[221] F. Eckermann, "ns-3_c-v2x: Cellular vehicle-to-everything (c-v2x) mode 4 model for ns-3." GitHub, https://github.com/FabianEckermann/ns-3_c-v2x.

[222] D. Gündüz, F. M. Van Der Meulen, and H. V. Poor, "Spoofing detection in the physical layer with graph neural networks," 2024.

[223] S. So, J. Petit, and D. Starobinski, "Physical layer plausibility checks for misbehavior detection in v2x networks," in *Proceedings of the 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'19)*, pp. 4:1–4:10, 2019. ACMISBN 978-1-4503-5933-7.

[224] X. Han, Y. Liu, and Z. Lu, "Defending against wi-fi spoofing attacks leveraging physical-layer features." https://usf.technologypublisher.com/technology/56025, 2025. Accessed: 2025-10-20; Tech ID: 24T033, University of South Florida.

[225] NTUMARS, "Awesome wifi csi sensing: A list of papers and resources on wifi csi sensing." https://github.com/NTUMARS/Awesome-WiFi-CSI-Sensing, 2024. Accessed: 2025-10-15.

[226] M. Authors, "V2x wireless technology identification using time–frequency analysis and random forest classifier," *Sensors (Basel)*, vol. 21, no. 13, p. 4492, 2021.

[227] M. Lichtman, "Usrp in python | pysdr: A guide to sdr and dsp using python." https://pysdr.org/content/usrp.html.

[228] MATLAB & Simulink, "What is software-defined radio (sdr)?." https://www.mathworks.com/discovery/sdr.html, 2024.

[229] welle.io, "Soapysdr." https://www.welle.io/devices/soapysdr.

[230] G. R. Wiki, "Soapy." https://wiki.gnuradio.org/index.php/Soapy.

[231] D. Packages, "Debian – details of package python3-soapysdr in buster." https://packages.debian.org/sid/sh4/python3-soapysdr.

[232] PothosWare, "Soapysdr: Vendor and platform neutral sdr support library." https://github.com/pothosware/SoapySDR.

[233] RTL-SDR, "Rtl-sdr platform." https://www.rtl-sdr.com/, 2024.

[234] Cyber Defense Magazine, "Software-defined radio for incident response." https://www.cyberdefensemagazine.com/software-defined-radio/, 2024.

[235] M. Wickert, "scikit-dsp-comm documentation," 2024.

[236] 3GPP, "Testing c-v2x access layer for its devices," 2024.

[237] A. Sharma *et al.*, "An optimized graph neural network-based approach for intrusion detection in smart vehicles," 2024.

[238] W. Aldosari, "Deep learning-based location spoofing attack detection and time-of-arrival estimation through power received in iot networks," *Sensors*, vol. 23, no. 23, p. 9606, 2023.

[239] University of South Florida, "Defending against wi-fi spoofing attacks leveraging physical-layer features," 2024.

[240] VIAVI Solutions Inc., "What is software defined radio (sdr)?." https://www.viavisolutions.com/en-us/what-software-defined-radio-sdr, 2024.

[241] Bliley Technologies, "10 popular software defined radios (sdrs) of 2022." https://blog.bliley.com/10-popular-software-defined-radios-sdr, 2024.

[242] G. Dong, M. Tang, Z. Wang, J. Gao, S. Guo, L. Cai, R. Gutierrez, B. Campbel, L. E. Barnes, and M. Boukhechba, "Graph neural networks in iot: A survey," *ACM Transactions on Sensor Networks*, vol. 19, no. 2, pp. 1–50, 2024.

[243] T. Bilot, N. E. Madhoun, K. A. Agha, and A. Zouaoui, "Graph neural networks for intrusion detection: A survey," *IEEE Access*, vol. 11, pp. 49114–49139, 2023.

[244] jwwthu, "Gnn-communication-networks: Graph-based deep learning for communication networks." https://github.com/jwwthu/GNN-Communication-Networks, 2024.

[245] P. G. Developers, "Colab notebooks and video tutorials - pytorch geometric - read the docs." Read the Docs, https://pytorch-geometric.readthedocs.io/en/2.6.1/get_started/colabs.html.

[246] G. Colaboratory, "3. graph classification.ipynb - colab." https://colab.research.google.com/drive/1I8a0DfQ3fI7Njc62__mVXUlcAleUclnb.

[247] H. Zhang *et al.*, "A multi-information fusion anomaly detection model based on convolutional neural networks and autoencoder," *Scientific Reports*, vol. 14, p. 15760, 2024.

[248] 3GPP, "3gpp releases 16, 17, 18 overview." https://www.3gpp.org/specifications-technologies/releases, 2024.

[249] Nokia Bell Labs, "5g releases 16 and 17 in 3gpp white paper," 2024. https://d1p0gxnqcu0lvz.cloudfront.net/documents/Nokia_Bell_Labs_5G_Releases_16_and_17_in_3GPP_White_Paper_1_EN.pdf.

[250] M. Fey and J. E. Lenssen, "Pytorch geometric: Library for deep learning on graphs,python library for geometric deep learning." https://pytorch-geometric.readthedocs.io/, 2024.

[251] Cavli Wireless, "Edge computing guide: Transforming real-time data processing." https://www.cavliwireless.com/blog/nerdiest-of-things/edge-computing-for-iot-real-time-data-and-low-latency-processing, 2024.

[252] TechTarget, "What is edge computing? everything you need to know." https://www.techtarget.com/searchdatacenter/definition/edge-computing, 2024.

[253] Microsoft Azure, "What is edge computing?." https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-edge-computing, 2024.

[254] N. Developers, "Tutorial – networkx 3.4.2 documentation." https://networkx.org/documentation/stable/tutorial.html.

[255] T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," in *International Conference on Learning Representations*, 2017.

[256] P. G. Developers, "Introduction by example – pytorch_geometric documentation." Read the Docs, https://pytorch-geometric.readthedocs.io/en/2.6.1/get_started/introduction.html.

[257] S. Developers, "Getting started - spektral." https://graphneural.network/getting-started/.

[258] TopBots, "Graph convolutional network implementation with the proteins benchmark dataset." https://www.topbots.com/graph-convolutional-network-implementation/.

[259] E. M. John Roar Ventura Solaas, Nilufer Tuptuk, "Systematic review: Anomaly detection in connected and autonomous vehicles." arXiv preprint arXiv:2405.02731, https://arxiv.org/html/2405.02731v1, 2024.

[260] SAE International, "Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles," April 2021.

[261] C. Miller and C. Valasek, "Adventures in automotive networks and control units," technical report, IOActive Labs Research, 2013. Presented at DEF CON 21, August 2013.

[262] "Nr; nr and ng-ran overall description; stage 2," Tech. Rep. Technical Specification 38.300, Release 16, 3rd Generation Partnership Project (3GPP), 2020. Available: https://www.3gpp.org/ftp/Specs/archive/38_series/38.300/.

[263] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of dsrc and cellular network technologies for v2x communications: A survey," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 9457–9470, 2016.

[264] A. Krayani, N. J. William, L. Marcenaro, and C. Regazzoni, "Jammer detection in vehicular V2X networks," in *Proceedings of the 2022 Microwave Mediterranean Symposium (MMS)*, (Pizzo Calabro, Italy), IEEE, May 2022.

[265] National Highway Traffic Safety Administration, "Cybersecurity best practices for the safety of modern vehicles," tech. rep., NHTSA, U.S. Department of Transportation, 2022.

[266] M. A. Rahman, S. W. Tan, M. S. Sohail, G. B. Gaggero, F. Patrone, M. Marchese, and P. Pillai, "Cybervehicare: A testbed for cybersecurity of vehicle to everything (v2x) automotive systems," in *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 818–823, 2025.

[267] M. M. Yamin, B. Katt, and V. Gkioulos, "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture," *Computers & Security*, vol. 88, p. 101636, 2020.

[268] N. Chouliaras, V. Katos, L. Maglaras, and H. Janicke, "Cyber ranges and testbeds for education, training, and research," *Applied Sciences*, vol. 11, no. 4, p. 1809, 2021.

[269] D. C. Ukwandu, M. A. Ferrag, L. Maglaras, H. Janicke, and A. Derhab, "A review of cyber-ranges and test-beds: Current and future trends," *Sensors*, vol. 20, no. 24, p. 7148, 2020.

[270] National Highway Traffic Safety Administration, "Vehicle cybersecurity training curriculum pilot testing," 2023. Accessed: 2024-10-05.

[271] European Union Agency for Cybersecurity (ENISA, "European union agency for cybersecurity (enisa)," 2024. Accessed: 2025-10-06.

[272] Automotive ISAC, "Automotive information sharing and analysis center (automotive isac)," 2025. Accessed: 2025-10-06.

[273] O. Pospišil, P. Blázek, K. V. Kuchař, R. Fujdiak, and J. Misurec, "Application perspective on cybersecurity testbed for industrial control systems," vol. 21, p. 8119, 2021.

[274] S. Mahmood, H. N. Nguyen, and S. A. Shaikh, "Automotive cybersecurity testing: Survey of testbeds and methods," in *Digital Transformation, Cyber Security and Resilience of Modern Societies*, pp. 219–243, Springer, 2021.

[275] D. Granata, M. Rak, and G. Salzillo, "Towards hybridgecan, a hybrid bridged can platform for automotive security testing," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 249–254, IEEE, 2021.

[276] C. E. Everett and D. McCoy, "{OCTANE}(open car testbed and network experiments): Bringing {Cyber-Physical} security research to researchers and students," in *6th Workshop on Cyber Security Experimentation and Test (CSET 13)*, 2013.

[277] T. Toyama, T. Yoshida, H. Oguma, and T. Matsumoto, "Pasta: portable automotive security testbed with adaptability," 2018.

[278] R. Caviglia, G. B. Gaggero, N. Vincis, O. Morando, A. Aceti, and M. Marchese, "Spat: A testbed for automotive cybersecurity training," in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 381–386, 2023.

[279] European Union Agency for Cybersecurity (ENISA), "Smart grid security: Recommendations for europe and member states," Tech. Rep. ENISA Report, European Union Agency for Cybersecurity (ENISA), July 2012. Accessed: 2025-10-22.

[280] European Union Agency for Cybersecurity (ENISA), "Eu incident response and cyber crisis management," tech. rep., 2025. Accessed: 2025-10-22.

[281] GNU Radio Community, "Gnu radio out-of-tree module template," 2023. Template for creating custom GNU Radio blocks.

[282] B. Bloessl, M. Segata, C. Sommer, and F. Dressler, "gr-ieee802-11: An ieee 802.11a/g/p ofdm transceiver for gnu radio," 2019. GNU Radio implementation of IEEE 802.11 standards.

Acknowledgments

This doctoral journey has been a truly transformative experience, made possible through the support, guidance, and encouragement of many remarkable individuals and institutions.

I would like to express my deepest gratitude to my supervisor, Professor Fabio Patrone, whose expertise, vision, and unwavering support have guided me throughout this research. His scientific insight and encouragement have been fundamental to the development of this thesis and to my growth as a researcher. I am sincerely grateful to Professor Fabio Patrone for his continuous support and assistance throughout the various challenges of my Ph.D. journey. Your guidance and encouragement during critical moments have been invaluable.

I extend my heartfelt thanks to AITEK S.p.A. for providing the industrial framework that enabled this research to bridge academic investigation with real world application. Working within an industrial context significantly strengthened the practical relevance of this work. In particular, I am profoundly thankful to my industrial coordinator, Stefano Deluchi and Marzia Pipi, for their continuous support, professional guidance, and for fostering a collaborative and stimulating working environment. I also wish to thank all my colleagues at AITEK S.p.A. for their cooperation, technical discussions, and team spirit, which enriched both the professional and personal dimensions of this experience.

I also extend my heartfelt thanks to the University of Wolverhampton for hosting me during my research period abroad. This experience significantly broadened my academic perspective and strengthened the international dimension of my work. In particular, I am profoundly thankful to Professor Dr Arafat ur Rehman for his mentorship, collaboration, and generous support during my time in the United Kingdom. His expertise and guidance greatly enriched my research, especially in advancing the experimental aspects of this work.

I would also like to acknowledge all colleagues and fellow doctoral researchers who contributed directly or indirectly to this journey. The stimulating discussions, collaborative environment, and shared challenges made this experience both intellectually rewarding and personally meaningful.

Finally, I express my deepest gratitude to my family for their unconditional love and unwavering belief in me. To my parents, thank you for instilling in me the value of education, perseverance, and integrity. Your sacrifices and encouragement have been the foundation of all my achievements. This thesis is the result of collective support, inspiration, and belief, for which I am profoundly thankful.

Muhammad Saad Sohail